

Faculdade de Engenharia da Universidade do Porto



**Gestão de uma Infra-Estrutura de Rede Wi-Fi com
recurso ao SNMP**

Carlos Filipe Almeida Mendonça

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

Orientador: Prof. João Neves

Julho de 2008

A Dissertação intitulada

“Gestão de uma Infra-Estrutura de Rede Wi-Fi com Recurso ao SNMP”

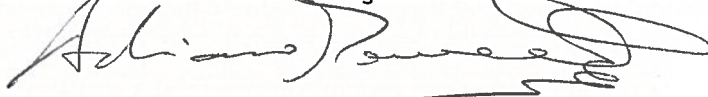
foi aprovada em provas realizadas 16/Julho/2008

o júri

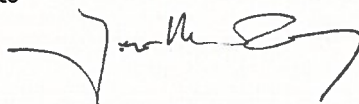
Presidente Professor Doutor Mário Jorge Moreira Leitão
Professor Associado da Faculdade de Engenharia da Universidade do Porto



Professor Doutor Adriano Jorge Cardoso Moreira
Professor Associado da Escola de Engenharia da Universidade do Minho



Professor Doutor João Manuel Couto das Neves
Professor Auxiliar Convocado 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 - Carlos Filipe Almeida Mendonça



Faculdade de Engenharia da Universidade do Porto

Resumo

Nestes últimos anos o uso da tecnologia de redes sem fios tem tido um crescimento enorme. Actualmente é possível encontrar infra-estruturas de rede Wi-Fi em variadíssimos locais, existindo a tendência de aumentar em tamanho e complexidade. Como tal, a importância da área de gestão de redes torna-se cada vez mais incontestável. A gestão de infra-estruturas deste tipo apresenta desafios não encontrados em tecnologias de rede com fios, sendo necessário o desenvolvimento de técnicas e ferramentas que permitam resolver os problemas de gestão específicos desta tecnologia de rede.

Abstract

In recent years the use of wireless network technology had an enormous growth. Nowadays it's possible to find Wi-Fi network infrastructures in many places. There is also a tendency to increase in size and complexity. As such, the importance of a network management system becomes unquestionable. The management of a network infrastructure like this presents challenges not found in wired network technologies, being necessary to develop tools and techniques to address the specific management problems of this network technology.

Agradecimentos

Este espaço é dedicado a todas as pessoas que deram a sua contribuição para que este trabalho fosse realizado.

Em primeiro lugar agradeço ao meu orientador, Professor João Neves, pela forma como orientou o meu trabalho. Agradeço também o esforço desenvolvido na leitura e sugestões de revisão deste documento.

Agradeço também à minha família que, de uma forma ou de outra, me apoiou.

Por último, agradeço a todos aqueles que não foram mencionados, mas que de alguma forma também contribuíram para a elaboração deste trabalho.

Carlos Mendonça

Índice

1 INTRODUÇÃO	1
1.1 TEMA	1
1.2 OBJECTIVO	2
1.3 ESTRUTURA DA DISSERTAÇÃO	2
2 REDES WI-FI	3
2.1 NORMA IEEE 802.11	3
2.1.1 ARQUITECTURA	4
2.1.2 CAMADA FÍSICA (PHY)	7
2.1.3 CAMADA DE ACESSO AO MEIO (MAC)	8
2.1.4 SEGURANÇA	11
2.2 NORMA IEEE 802.1X	12
2.2.1 ARQUITECTURA	12
3 PROTOCOLO SNMP E GESTÃO DE REDES	13
3.1 PROTOCOLO SNMP	13
3.1.1 ARQUITECTURA	14
3.1.2 INFORMAÇÃO DE GESTÃO	16
3.1.3 PROTOCOLO DE GESTÃO	27
3.2 GESTÃO DE REDES	36
3.2.1 ÁREAS FUNCIONAIS	36
3.2.2 SOLUÇÕES EXISTENTES	39
4 CARACTERIZAÇÃO DO PROBLEMA	43
4.1 IDENTIFICAÇÃO DOS PRINCIPAIS PROBLEMAS DE GESTÃO E OPERAÇÃO	43
4.1.1 MONITORIZAÇÃO DO DESEMPENHO	43
4.1.2 CONTABILIZAÇÃO	44
4.1.3 MONITORIZAÇÃO DA SEGURANÇA	44
4.1.4 DETECÇÃO DE FALHAS	44

4.1.5	CONFIGURAÇÃO	45
4.2	ANÁLISE DAS MIBS	47
4.2.1	MIB-II	47
4.2.2	MIB GENÉRICA IEEE 802.11	51
4.2.3	MIBS PROPRIETÁRIAS	55
5	IMPLEMENTAÇÃO	63
5.1	LOCALIZAÇÃO DA SOLUÇÃO NA REDE WI-FI	63
5.2	TECNOLOGIAS ESCOLHIDAS PARA A IMPLEMENTAÇÃO DA SOLUÇÃO	65
5.3	ARQUITECTURA DO SISTEMA DE GESTÃO	66
5.3.1	MÓDULO DE GESTÃO DE OBJECTOS PRESENTES NA MIB-II	69
5.3.2	MÓDULO DE GESTÃO DE OBJECTOS RELACIONADOS COM A NORMA IEEE 802.11	72
5.3.3	CLASSIFICADOR DE NOTIFICAÇÕES	79
5.3.4	RECOLHA PERIÓDICA DE INFORMAÇÃO	81
5.3.5	SERVIDOR AAA	85
5.3.6	INTERFACE COM O UTILIZADOR	87
5.4	SEGURANÇA DA SOLUÇÃO	95
5.4.1	PROTOCOLO SNMP	95
5.4.2	PROTOCOLO TELNET	95
5.4.3	PROTOCOLO RADIUS	96
6	CONCLUSÕES	97
6.1	SÍNTESE DO TRABALHO DESENVOLVIDO	97
6.2	DESENVOLVIMENTO FUTURO	98
	REFERÊNCIAS	99

Lista de figuras

Figura 2.1 - Localização da norma IEEE 802.11 no modelo de referência OSI.....	4
Figura 2.2 - Rede Wi-Fi em modo de Infra-estrutura.....	5
Figura 2.3 - Rede Wi-Fi em modo <i>Ad-hoc</i>	6
Figura 2.4 - Normas IEEE 802.11 para a camada física.....	8
Figura 2.5 - Formato de uma trama MAC da norma IEEE 802.11	9
Figura 2.6 - Formato do campo de controlo de uma trama MAC da norma IEEE 802.11	10
Figura 2.7 - Arquitectura da norma IEEE 802.1X	12
Figura 3.1 - Arquitectura do protocolo SNMP	15
Figura 3.2 - Árvore de objectos definidos na SMIv1	17
Figura 3.3 - Árvore com o ramo enterprises	18
Figura 3.4 - Árvore de objectos definidos na SMIv2	22
Figura 3.5 - Árvore com os principais objectos da MIB-II	25
Figura 3.6 - PDU de uma mensagem SNMP	27
Figura 3.7 - Variable Bindings presente nos PDUs SNMP	28
Figura 3.8 - PDU SNMPv1 das operações GetRequest, GetNextRequest e SetRequest	28
Figura 3.9 - PDU SNMPv1 da operação GetResponse	29
Figura 3.10 - PDU SNMPv1 da operação Trap	30
Figura 3.11 - PDU SNMPv2 da operação GetBulkRequest	31
Figura 3.12 - PDU SNMPv2 da operação InformRequest.....	31
Figura 3.13 - PDU SNMPv2 da operação SNMPv2-Trap.....	32
Figura 3.14 - Arquitectura SNMPv3.....	34
Figura 3.15 - Interface de gestão da plataforma <i>AirWave Management Platform</i>	40
Figura 3.16 - Interface de gestão da plataforma <i>ManageEngine WiFi Manager</i>	40
Figura 4.1 - Objectos importantes da MIB-II	47
Figura 4.2 - Principais ramos da MIB IEEE802Dot11.....	51
Figura 4.3 - Ramo dot11smt da MIB IEEE802Dot11.....	52
Figura 4.4 - Ramo dot11mac da MIB IEEE802Dot11	53
Figura 4.5 - Ramo dot11res da MIB IEEE802Dot11	53

Figura 4.6 - Ramo dot11phy da MIB IEEE802Dot11	54
Figura 4.7 - Localização das MIBs proprietárias da Cisco na árvore de gestão.....	55
Figura 4.8 - Principais objectos da MIB CISCO-DOT11-IF-MIB	56
Figura 4.9 - Principais objectos da MIB CISCO-DOT11-SSID-SECURITY-MIB.....	57
Figura 4.10 - Principais objectos da MIB CISCO-DOT11-ASSOCIATION-MIB	58
Figura 4.11 - Principais objectos da MIB CISCO-CONFIG-COPY-MIB	60
Figura 4.12 - Principais ramos da MIB dos pontos de acesso da DLink.....	61
Figura 5.1 - Diagrama com a topologia da rede.....	63
Figura 5.2 - Arquitectura geral do sistema de gestão.....	66
Figura 5.3 - Detalhe do módulo de tratamento da informação.....	67
Figura 5.4 - Fluxograma do funcionamento do Classificador de notificações.....	79
Figura 5.5 - Modelo relacional das tabelas utilizadas pelo módulo Classificador de notificações	80
Figura 5.6 - Tabela utilizada pelo módulo de monitorização dos equipamentos	82
Figura 5.7 - Tabela utilizada pelo módulo de recolha da tabela de ARP dos routers	83
Figura 5.8 - Fluxograma do tratamento de cada entrada da tabela de ARP	83
Figura 5.9 - Tabela utilizada pelo módulo de recolha da lista de estações associadas.....	84
Figura 5.10 - Fluxograma do tratamento de cada associação a um ponto de acesso	84
Figura 5.11 - Diagrama de sequência com as mensagens de contabilização do protocolo RADIUS	86
Figura 5.12 - Página inicial da aplicação.....	87
Figura 5.13 - Página que permite adicionar equipamento	88
Figura 5.14 - Página onde são mostrados os detalhes de um AP	89
Figura 5.15 - Página onde são mostrados os detalhes de um <i>switch</i>	90
Figura 5.16 - Página onde é possível visualizar um histórico de eventos	91
Figura 5.17 - Página onde é possível observar o histórico de várias leituras de um AP	92
Figura 5.18 - Página que contem o histórico da movimentação de uma estação.....	93
Figura 5.19 - Página onde é possível observar os consumos de todos os utilizadores	94
Figura 5.20 - Página onde é possível visualizar os detalhes das várias sessões de um utilizador	94

Lista de tabelas

Tabela 2.1 - Combinações dos campos de endereços na trama MAC da norma IEEE 802.11	9
Tabela 4.1 - Tabela ifTable da MIB-II	48
Tabela 4.2 - Tabela atTable da MIB-II	50
Tabela 4.3 - Tabela ipNetToMediaTable da MIB-II	50
Tabela 5.1 - Métodos implementados no módulo MIB-II	69
Tabela 5.2 - Métodos que deverão ser implementados pelos módulos de adaptação ao fabricante.....	72

Lista de abreviaturas e siglas

AAA	<i>Authentication, Authorization and Accounting</i>
ACK	<i>Acknowledgment</i>
AES	<i>Advanced Encryption Standard</i>
AP	<i>Access Point</i>
ARP	<i>Address Resolution Protocol</i>
ASCII	<i>American Standard Code for Information Interchange</i>
ASN.1	<i>Abstract Syntax Notation One</i>
BER	<i>Basic Encoding Rules</i>
BSS	<i>Basic Service Set</i>
CCITT	<i>International Telegraph and Telephone Consultative Committee</i>
CLI	<i>Command Line Interface</i>
CRC	<i>Cyclic Redundancy Check</i>
CSMA/CA	<i>Carrier Sense Multiple Access with Collision Avoidance</i>
CSMA/CD	<i>Carrier Sense Multiple Access with Collision Detection</i>
CTS	<i>Clear To Send</i>
DCF	<i>Distributed Coordination Function</i>
DS	<i>Distribution System</i>
DSSS	<i>Direct Sequence Spread Spectrum</i>
DoD	<i>United States Department of Defense</i>
ESS	<i>Extended Service Set</i>
IANA	<i>Internet Assigned Numbers Authority</i>
IBSS	<i>Independent Basic Service Set</i>
ICMP	<i>Internet Control Message Protocol</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IETF	<i>Internet Engineering Task Force</i>
IP	<i>Internet Protocol</i>
ISM	<i>Industrial, Scientific and Medical</i>
ISO	<i>International Organization for Standardization</i>

ITU	<i>International Telecommunication Union</i>
FCS	<i>Frame Check Sequence</i>
FHSS	<i>Frequency Hopping Spread Spectrum</i>
LAN	<i>Local Area Network</i>
LLC	<i>Logical Link Control</i>
MAC	<i>Medium Access Control</i>
MIB	<i>Management Information Base</i>
NAS	<i>Network Access Server</i>
OFDM	<i>Orthogonal Frequency Division Multiplexing</i>
OID	<i>Object Identifier</i>
OSI	<i>Open Systems Interconnection</i>
PCF	<i>Point Coordination Function</i>
PDU	<i>Protocol Data Unit</i>
PHY	<i>Physical Layer</i>
RADIUS	<i>Remote Authentication Dial In User Service</i>
RFC	<i>Request for Comments</i>
RMON	<i>Remote Network Monitoring</i>
RTS	<i>Request To Send</i>
SGBD	<i>Sistema de Gestão de Bases de Dados</i>
SGMP	<i>Simple Gateway Monitoring Protocol</i>
SMI	<i>Structure of Managed Information</i>
SNMP	<i>Simple Network Management Protocol</i>
SNR	<i>Signal to Noise Ratio</i>
SSH	<i>Secure Shell</i>
SSID	<i>Service Set Identifier</i>
STA	<i>Station</i>
UDP	<i>User Datagram Protocol</i>
TCP	<i>Transmission Control Protocol</i>
TKIP	<i>Temporal Key Integrity Protocol</i>
VLAN	<i>Virtual Local Area Network</i>
WEP	<i>Wired Equivalent Privacy</i>
WLAN	<i>Wireless Local Area Network</i>
WPA	<i>Wi-Fi Protected Access</i>

Capítulo 1

Introdução

Este capítulo pretende fornecer uma visão global do trabalho desenvolvido e reportado na presente dissertação. Após uma breve exposição do tema abordado, são descritos os objectivos e, por último, é apresentada a estrutura da dissertação.

1.1 Tema

As redes sem fios baseadas na norma IEEE 802.11, geralmente conhecidas por redes Wi-Fi, têm sofrido uma grande expansão, sendo actualmente a tecnologia de redes sem fios mais utilizada. Devido às várias vantagens que esta tecnologia oferece é cada vez mais utilizada por empresas em detrimento de uma infra-estrutura com fios. A primeira das vantagens é a facilidade de instalação da própria infra-estrutura, pois não é necessário instalar tomadas de rede para os utilizadores ligarem os seus terminais. Outro ponto positivo para as redes sem fios é a mobilidade, pois permite que um utilizador se movimente mantendo a conectividade à rede, potenciando assim um aumento de produtividade. A escalabilidade também é uma vantagem deste tipo de redes, sendo esta bastante elevada devido à possibilidade serem adicionados pontos de acesso adicionais que permitem um aumento da capacidade da rede assim como uma ampliação da área de cobertura da rede. Também devido às várias melhorias efectuadas à norma base das redes Wi-Fi, pelos vários grupos de trabalho criados pelo IEEE, a capacidade destas redes têm sofrido um grande aumento.

Devido a todas estas vantagens, o aumento em número e complexidade de redes deste tipo obriga a que existam plataformas de gestão de forma a garantir o bom funcionamento das infra-estruturas de rede. Este tipo de redes cria novos desafios às plataformas de gestão pois passam a existir problemas que não existiam em redes com fios, requerendo novas soluções de gestão.

Para a gestão de redes foram desenvolvidos vários protocolos, mas nenhum conseguiu a implantação que o protocolo SNMP (*Simple Network Management Protocol*) tem actualmente. Esta vantagem do protocolo SNMP deveu-se não só à sua simplicidade, mas também por ter sido o primeiro a ser implementado, levando a que a maioria dos fabricantes de *hardware* e *software* o suportasse.

1.2 Objectivo

É objectivo desta dissertação a identificação dos principais problemas de operação e gestão de uma infra-estrutura de rede Wi-Fi e respectivo desenvolvimento de propostas de solução, usando o protocolo de gestão de redes SNMP, para uma plataforma de gestão integrada. De forma a ser demonstrado o cumprimento destes objectivos será desenvolvido um protótipo de uma plataforma de gestão com recurso a ferramentas de domínio público.

1.3 Estrutura da dissertação

Esta dissertação encontra-se organizada em seis capítulos.

O segundo capítulo tem como objectivo fazer uma introdução às redes Wi-Fi.

No terceiro capítulo é incluída uma apresentação do protocolo de gestão redes SNMP (*Simple Network Management Protocol*), uma pequena introdução à gestão de redes e uma comparação entre algumas soluções existentes para a gestão de redes Wi-Fi.

O quarto capítulo, Caracterização do Problema, apresenta a identificação de alguns dos problemas de operação e gestão de infra-estruturas deste tipo, assim como uma análise de algumas MIBs (*Management Information Base*).

O quinto capítulo, Implementação, descreve a solução implementada de forma a resolver os problemas descritos no capítulo anterior.

O sexto capítulo, Conclusões, apresenta uma síntese do trabalho desenvolvido e as melhorias que podem ser introduzidas em desenvolvimentos futuros nesta área.

Segue-se uma lista de todas as referências utilizadas no desenvolvimento deste trabalho.

Capítulo 2

Redes Wi-Fi

Neste capítulo é realizada uma breve apresentação sobre as redes baseadas na norma IEEE 802.11 (Redes Wi-Fi). É ainda incluído um pequeno tópico onde é apresentada a norma IEEE 802.1X de uma forma muito sumária.

2.1 Norma IEEE 802.11

A norma IEEE 802.11 [1], norma base das redes Wi-Fi, fornece as especificações que permitem a conectividade entre estações sem fios e infra-estruturas de redes cabladas. Tal como as outras normas da família IEEE 802, esta norma também define as especificações da camada física (PHY), nível 1 do modelo de referência OSI, e as especificações da camada de controlo de acesso ao meio (MAC). O nível 2 do modelo de referência OSI, a camada de ligação de dados, é a combinação da camada de controlo de acesso ao meio e a camada de controlo da ligação lógica (LLC), especificada na norma IEEE 802.2.

De forma a ilustrar a localização da norma IEEE 802.11 no modelo de referência OSI segue-se a seguinte imagem.

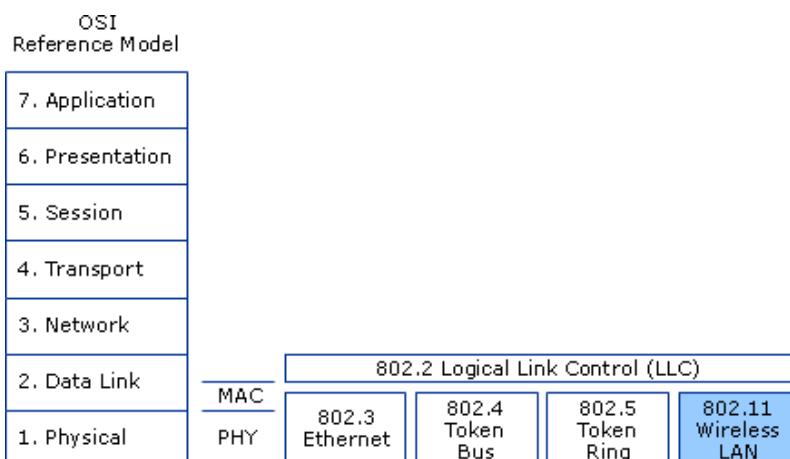


Figura 2.1 - Localização da norma IEEE 802.11 no modelo de referência OSI

2.1.1 Arquitectura

A arquitectura da norma IEEE 802.11 consiste em vários componentes que interagem de forma a que seja possível a formação de uma rede local sem fios com suporte de mobilidade de estações de uma forma transparente para as camadas superiores. Os seus componentes são apresentados a seguir:

- **AP (Access Point)** - São estações análogas às estações base das redes de comunicação móveis, permitindo a operação da rede no modo de infra-estrutura.
- **STA (Station)** - É qualquer dispositivo que implemente as camadas física e de acesso ao meio da norma IEEE 802.11. Por exemplo um interface de rede Wi-Fi de um computador.
- **BSS (Basic Service Set)** - Representa um grupo de estações que estão sob o controlo de um AP, utilizando o modo de operação denominado de Infra-estrutura.
- **IBSS (Independent Basic Service Set)** - Representa um grupo de estações que não utilizam a estrutura de comunicação fornecida pelo AP. As estações comunicam directamente umas com as outras. Este modo de operação é denominado de *Ad-hoc*.
- **DS (Distribution System)** - É um meio pela qual os APs comunicam entre si. A norma IEEE 802.11 não especifica a tecnologia deste sistema, podendo ser baseado em qualquer tecnologia de rede, sendo a mais comum a tecnologia *Ethernet*.
- **ESS (Extended Service Set)** - Representa um conjunto de BSSs interligados através de um sistema de distribuição (DS). A possibilidade de interligar vários

BSSs permite aumentar a área de cobertura, levando a que seja possível uma maior mobilidade das estações.

- **Portal** - É a entidade que interliga o sistema de distribuição a outros tipos de redes. Se a outra rede for da família IEEE 802.X, a função desta entidade é semelhante a uma *bridge*.

Segue-se uma ilustração de uma rede Wi-Fi em modo de infra-estrutura com dois BSSs interligados por um sistema de distribuição, formando assim um ESS. Por sua vez o sistema de distribuição está ligado a um portal que permite o acesso a uma rede da família IEEE 802.X.

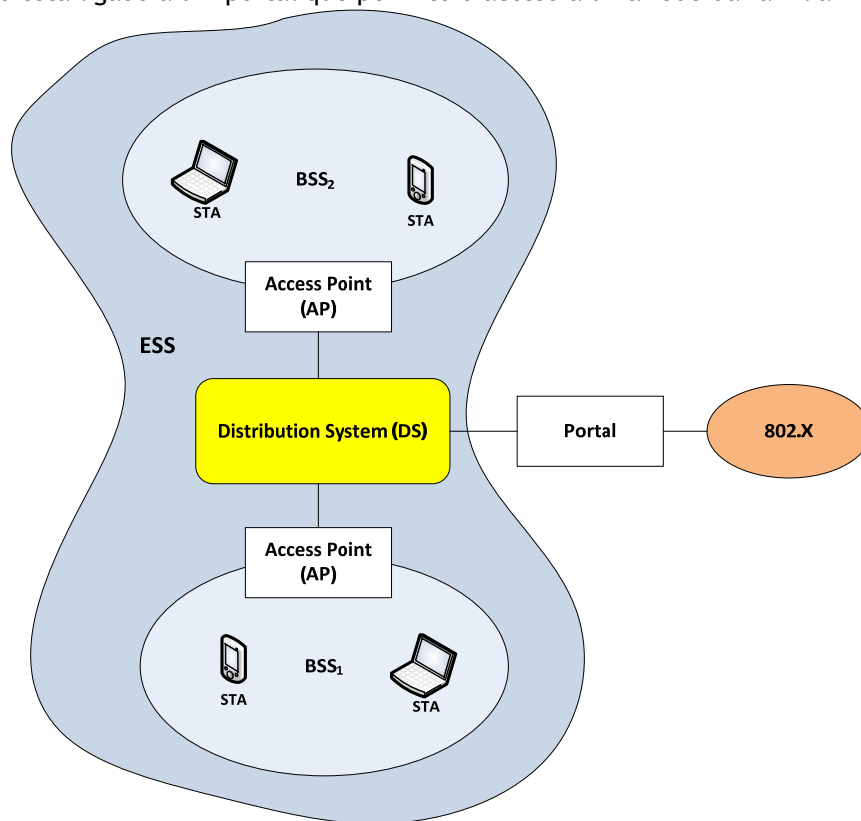


Figura 2.2 - Rede Wi-Fi em modo de Infra-estrutura

Na figura seguinte é possível observar uma rede Wi-Fi em modo *Ad-hoc* constituída por 4 estações. Neste modo as estações comunicam directamente umas com as outras.

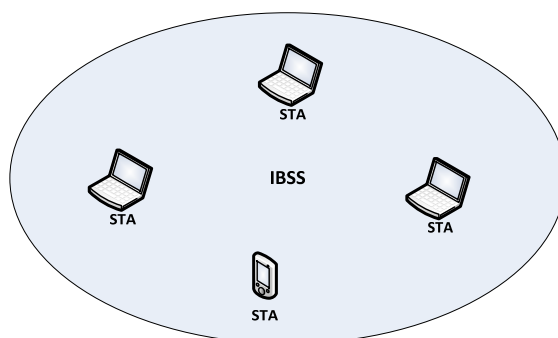


Figura 2.3 - Rede Wi-Fi em modo *Ad-hoc*

Em qualquer um dos modos de operação a rede é identificada pelo nome dado pelo SSID (*Service Set Identifier*).

2.1.2 Camada Física (PHY)

Nas especificações da camada física são definidas técnicas de espalhamento de espectro que permitem a operação de várias estações em simultâneo sobre a mesma banda de frequências com o mínimo de interferência entre elas. Na norma base é definida a utilização da técnica de espalhamento de espectro por salto em frequência (FHSS) assim como a técnica de espalhamento de espectro por sequência directa (DSSS), sobre uma das bandas ISM (*Industrial, Scientific and Medical*), operando entre 2,4GHz e 2,5GHz.

A norma especifica um débito de 2Mb/s que pode ser reduzido para 1Mb/s em condições menos ideais. Estes débitos comparados com os débitos obtidos em redes Ethernet são baixos. Então de forma a aumentar o débito, o IEEE criou os seguintes grupos de trabalho:

- **IEEE 802.11b [2]** - Esta norma foi a principal melhoria criada para a norma base, pois permitiu um aumento do débito para 11Mb/s em condições ideais, podendo ser utilizados débitos menores de 5,5Mb/s, 2Mb/s ou 1Mb/s conforme as condições de transmissão. Utiliza a técnica de espalhamento de espectro por sequência directa (DSSS) e funciona sob a mesma banda de frequências usadas na norma base.
- **IEEE 802.11a [3]** - Esta norma permitiu o aumento do débito para 54Mb/s em condições ideais à custa do uso da técnica OFDM (*Orthogonal Frequency Division Multiplexing*), onde o espectro é dividido em múltiplas portadoras (52 no total) de pequena largura de banda, permitindo uma maior resistência à interferência. Em condições menos ideais o débito pode ser reduzido para 48Mb/s, 36Mb/s, 24Mb/s, 18Mb/s, 12Mb/s, 9Mb/s ou 6Mb/s. A banda de frequências de operação é diferente das outras normas, utilizando outra das bandas ISM em 5GHz. A implementação desta norma demorou, nunca tendo grande aceitação devido à larga implantação de produtos compatíveis com a norma IEEE 802.11b.
- **IEEE 802.11g [4]** - Esta norma tal como a IEEE 802.11a, permite um débito máximo de 54Mb/s usando a banda de frequências entre 2,4GHz e 2,5GHz em conjunto com a técnica OFDM. Outra das vantagens desta norma é a compatibilidade com a IEEE 802.11b e a coexistência de redes com estas duas normas. Isto foi necessário visto que já existia uma larga implementação de redes Wi-Fi baseadas na norma IEEE 802.11b. Em condições menos ideais o débito pode ser reduzido para 48Mb/s, 36Mb/s, 24Mb/s, 18Mb/s, 12Mb/s ou 6Mb/s.

Actualmente está em desenvolvimento a norma IEEE 802.11n que tira partido da tecnologia MIMO (*Multiple Input Multiple Output*) para aumentar o débito.

Segue-se uma imagem que resume as características principais das várias normas.

	802.2 Logical Link Control (LLC)			
MAC	CSMA/CA			
PHY	802.11 2 Mbps S-Band ISM FHSS	802.11b 11 Mbps S-Band ISM DSSS	802.11a 54 Mbps C-Band ISM OFDM	802.11g 54 Mbps S-Band ISM OFDM

Figura 2.4 - Normas IEEE 802.11 para a camada física

2.1.3 Camada de Acesso ao Meio (MAC)

A camada de acesso ao meio especifica a utilização de três métodos de acesso ao meio:

- DCF (*Distributed Coordination Function*) com CSMA/CA
- DCF (*Distributed Coordination Function*) com RTS/CTS
- PCF (*Point Coordination Function*)

O mecanismo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) ao contrário do mecanismo usado nas redes IEEE 802.3 (Ethernet), CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), não detecta as colisões, apenas as tenta evitar através da espera de um tempo aleatório após a detecção que o meio está livre.

A camada MAC também é responsável pela fragmentação e posterior reconstituição das tramas, sendo este processo transparente para as camadas superiores. A possibilidade de fragmentar a trama é importante porque minimiza a probabilidade de erro em situações onde o SNR (*Signal to Noise Ratio*) é baixo.

2.1.3.1 Tramas MAC

Os três tipos de tramas utilizados são os seguintes:

- **Tramas de Dados** - Utilizadas para transmissão de dados.
- **Tramas de Controlo** - Utilizadas para o controlo de acesso ao meio (RTS, CTS, e ACK).
- **Tramas de Gestão** - Utilizadas para troca de informação de gestão.

A figura seguinte apresenta o formato de uma trama MAC, sendo esta composta por um cabeçalho (*MAC Header*), pelo conteúdo (*Frame Body*) e por um campo utilizado para verificação de redundância cíclica (*Frame Check Sequence*).

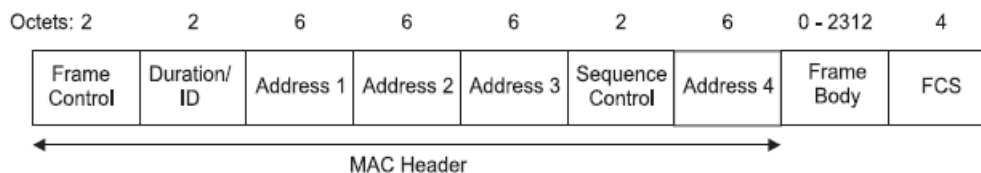


Figura 2.5 - Formato de uma trama MAC da norma IEEE 802.11

Cabeçalho MAC

- *Duration/ID* - Nas tramas do tipo *Power Save Poll* o campo contém a identidade da associação da estação emissora. Nos outros tipos de tramas indica a duração até à transmissão da próxima trama.
- **Campos de Endereço** (*Address 1*, *Address 2*, *Address 3*, *Address 4*) - Combinação dos seguintes tipos de endereços:
 - *BSSID* - No caso de uma rede em modo de Infra-estrutura é o endereço MAC do AP. No caso de uma rede em modo *Ad-hoc* é o endereço MAC alocado pela estação que cria a rede.
 - *Destination Address (DA)* - Endereço MAC da estação de destino final da trama.
 - *Source Address (SA)* - Endereço MAC da estação que criou a trama.
 - *Receiver Address (RA)* - Endereço MAC da próxima estação a receber a trama.
 - *Transmitter Address (TA)* - Endereço MAC da estação que emitiu a trama.

Tabela 2.1 - Combinações dos campos de endereços na trama MAC da norma IEEE 802.11

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

- *Sequence Control* - Este campo é composto pelos seguintes 2 campos:

- o **Sequence Number (12 bit)** - Indica o número de sequência de cada trama, sendo igual em todas as tramas fragmentadas. É incrementado até ao seu valor máximo (4095).
- o **Fragment Number (4 bit)** - Indica o número do fragmento no caso das tramas fragmentadas. Inicia no valor zero.

O Campo **FCS (Frame Check Sequence)** é um **CRC (Cyclic Redundancy Check)** calculado sobre todos os campos do cabeçalho e conteúdo da trama. É utilizado para a estação receptora verificar a integridade da trama.

O campo **Frame Control** é composto pelos seguintes campos ou *flags*:

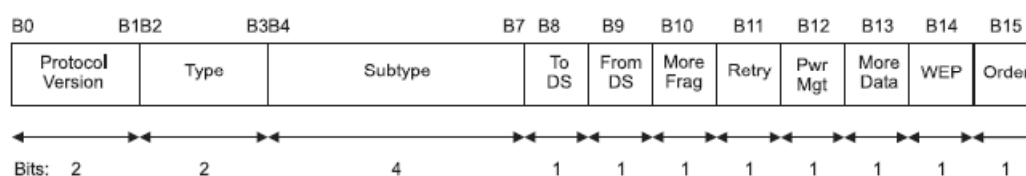


Figura 2.6 - Formato do campo de controlo de uma trama MAC da norma IEEE 802.11

- **Protocol Version** - Identifica a versão do protocolo usada. As estações usam este campo para determinar se deverão ou não descartar a trama.
- **Type** - Indica o tipo de trama: Trama de Dados, Trama de Controlo ou Trama de Gestão.
- **Subtype** - Indica o subtipo da trama.
- **To DS** - Toma o valor 1 em tramas destinadas ao sistema de distribuição.
- **From DS** - Toma o valor 1 em tramas com origem no sistema de distribuição.
- **More Frag** - Indica que irão chegar mais fragmentos pertencentes a esta trama.
- **Retry** - Indica que a trama é de uma retransmissão.
- **Pwr Mgt** - Indica se a estação que enviou a trama está no modo de baixo consumo (*Power Save*).
- **More Data** - Indica a uma estação que se encontra em modo de baixo consumo (*Power Save*) que virão mais tramas.
- **WEP** - Indica que o conteúdo da trama está encriptado.
- **Order** - Indica que as tramas recebidas terão que ser processadas pelo seu número de sequência.

2.1.4 Segurança

Devido ao canal de comunicação compartilhado das redes Wi-Fi, a segurança destas é algo que não pode ser desprezado. Como tal a seguir são brevemente apresentados os três protocolos de segurança utilizados.

2.1.4.1 WEP (Wired Equivalent Privacy)

O protocolo WEP foi o algoritmo de encriptação originalmente especificado na norma IEEE 802.11. Desde logo foram descobertos problemas de segurança, permitindo de uma forma relativamente fácil descobrir a chave.

2.1.4.2 WPA (Wi-Fi Protected Access)

O WPA é um protocolo de segurança introduzido nas redes Wi-Fi para resolver os problemas do WEP. Foi lançado pela Wi-Fi Alliance enquanto a norma IEEE 802.11i não estava completamente finalizada. O protocolo WPA utiliza o algoritmo de encriptação TKIP (*Temporal Key Integrity Protocol*). Também permite de uma forma opcional o uso do algoritmo AES (*Advanced Encryption Standard*) para encriptação.

Possui os seguintes dois modos de operação:

- **WPA-Personal** - A autenticação é realizada através de uma chave que foi partilhada entre os vários intervenientes (*Pre-Shared Key* - PSK).
- **WPA-Enterprise** - A autenticação é realizada através de um servidor de autenticação (com recurso à norma IEEE 802.1X), sendo normalmente utilizada em redes empresariais.

2.1.4.3 WPA2 (Wi-Fi Protected Access 2)

O protocolo WPA2, baseado na norma IEEE 802.11i [5] final, foi desenvolvido para substituir formalmente o protocolo WEP. Ao contrário do protocolo WPA onde o uso do algoritmo AES era opcional, neste é obrigatório. Também possui os mesmos dois modos de operação encontrados no WPA.

2.2 Norma IEEE 802.1X

A norma IEEE 802.1X [6] define um protocolo de controlo de acessos à rede por porta. Foi desenvolvida para a família de redes IEEE 802, sendo bastante utilizada em redes Wi-Fi empresariais.

2.2.1 Arquitectura

A arquitectura do protocolo IEEE 802.1X é baseada nas seguintes entidades:

- **Authenticator** - Equipamento que fornece o serviço de rede. No caso de redes Wi-Fi normalmente é um AP.
- **Supplicant** - Cliente.
- **Authentication Server** - Entidade que fornece o serviço de autenticação à entidade *Authenticator*. Este serviço determina se as credenciais fornecidas pelo *Supplicant* estão autorizadas a usar o serviço de rede. Pode ser por exemplo um servidor RADIUS (*Remote Authentication Dial In User Service*).

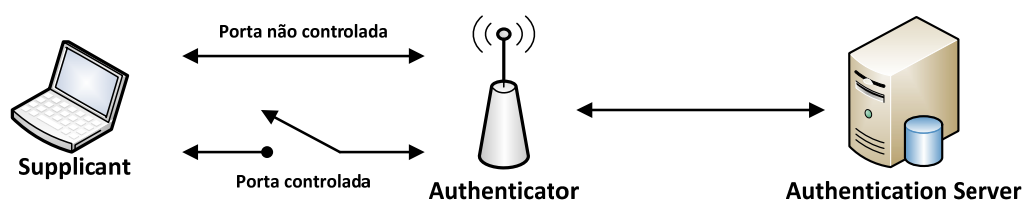


Figura 2.7 - Arquitectura da norma IEEE 802.1X

Durante a fase de autenticação apenas é permitido o tráfego 802.1X entre o *Supplicant* e o *Authenticator*, usando a porta não controlada. Após uma autenticação positiva a porta controlada é aberta passando a ser possível o fluxo de outro tipo de tráfego.

Após esta fase é possível a troca de chaves entre o *Authenticator* e o *Supplicant* para a cifra de tramas entre estas duas entidades.

Capítulo 3

Protocolo SNMP e Gestão de Redes

Neste capítulo é efectuada uma apresentação do protocolo SNMP (*Simple Network Management Protocol*). É ainda incluído um breve tópico sobre gestão de redes onde é feita uma análise comparativa entre algumas das soluções existentes para a gestão de redes Wi-Fi.

3.1 Protocolo SNMP

O SNMP (*Simple Network Management Protocol*) é um conjunto de especificações, desenvolvidas pelo IETF (*Internet Engineering Task Force*), com o objectivo de tornar possível a gestão de redes utilizando um protocolo simples e normalizado. Foi inicialmente desenvolvido para funcionar sobre o modelo TCP/IP e como tal foi considerado como uma solução para curto prazo, visto que na altura pensava-se que o modelo de redes OSI acabaria por substituir o modelo TCP/IP. O anterior protocolo que apenas permitia a gestão de *gateways*, o SGMP (*Simple Gateway Monitoring Protocol*), foi rapidamente substituído pelo SNMP e hoje em dia o SNMP é a solução dominante para a gestão de redes devido ao progresso lento do modelo de redes OSI e consequentemente o seu protocolo de gestão.

Na sua especificação base é incluída a definição da arquitectura do modelo de gestão, a definição das estruturas de dados e o protocolo de comunicação.

Ao longo dos anos houve uma evolução das especificações do protocolo, levando à existência de três versões, sendo que actualmente a versão mais recente é o SNMPv3.

A versão 2 do protocolo (SNMPv2) surgiu para resolver algumas das limitações encontradas na versão anterior e a versão 3 para resolver os problemas de segurança encontrados nas duas anteriores versões.

Embora o SNMPv3 seja o mais evoluído, a sua adopção por parte de alguns fabricantes de *hardware* e *software* tem sido lenta, levando a que actualmente o SNMPv2 ainda seja o mais utilizado.

3.1.1 Arquitectura

O modelo de gestão de redes SNMP é composto pelos seguintes elementos chave:

- **Estação de Gestão** - A Estação de Gestão é responsável por fazer o interface entre o gestor da rede e o sistema de gestão de rede. Poderá ser um componente isolado ou ser implementado num sistema partilhado. No mínimo terá que incluir:
 - Um interface onde o gestor da rede poderá monitorizar e controlar os elementos de rede.
 - Um base de dados de informação onde é incluída toda a informação de gestão de todas as entidades da rede.
 - Um conjunto de aplicações de gestão para análise de dados e recuperação de falhas.
- **Agente** - O Agente está presente nos equipamentos a serem geridos. É responsável por responder a pedidos enviados pela estação de gestão, mas pode também enviar para a estação de gestão, de uma forma assíncrona, informação importante que não tenha sido previamente solicitada por esta. De uma forma adicional pode também receber, da estação de gestão, pedidos de alteração de valores no equipamento sendo responsável por executar essa alteração e retornar o resultado.
- **Informação de Gestão** - A Informação de Gestão é composta por um conjunto de objectos que representam os recursos de cada elemento da rede. Na prática cada objecto é normalmente uma variável que representa um aspecto do equipamento gerido. De forma a agrupar um conjunto de objectos comuns a uma determinada categoria de equipamentos foram criados uns conjuntos de objectos designados por MIB (*Management Information Base*). Por exemplo, para o caso das *bridges* existem um conjunto de MIBs que são usadas para a gestão das mesmas.

- **Protocolo de Gestão** - O Protocolo de Gestão é utilizado na comunicação entre a estação de gestão e os agentes situados nos equipamentos. Este protocolo utiliza a pilha protocolar TCP/IP, utiliza o protocolo UDP (*User Datagram Protocol*) para transporte e está localizado ao nível da aplicação. As principais funcionalidades genéricas suportadas são:
 - `get` - Permite à estação de gestão obter o valor de um determinado objecto de um agente.
 - `set` - Permite à estação de gestão definir um valor para um determinado objecto num agente.
 - `trap` - Permite um agente notificar a estação de gestão para eventos importantes.

Segue-se uma ilustração que mostra de uma forma gráfica a interacção entre os vários elementos quem compõem a arquitectura do protocolo.

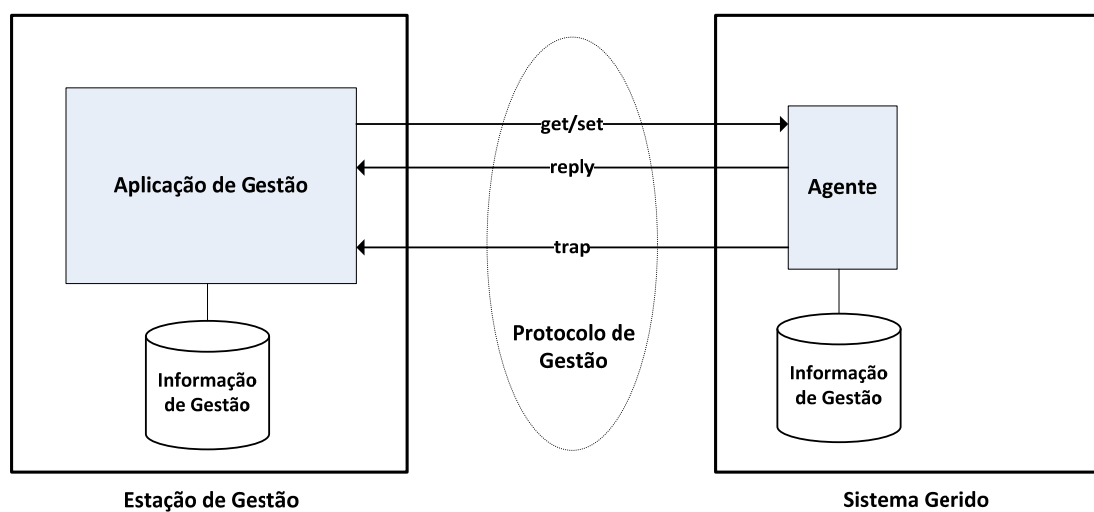


Figura 3.1 - Arquitectura do protocolo SNMP

3.1.2 Informação de Gestão

A Informação de Gestão é composta por um conjunto de objectos que representam os recursos de cada elemento da rede.

A forma como os objectos de gestão são definidos [7] é dada pela SMI (*Structure of Management Information*). A definição base dos objectos é composta pelos seguintes atributos:

- **Nome** - Identificador do objecto - OID (*Object Identifier*).
- **Sintaxe** - O tipo de cada objecto é definido usando a linguagem ASN.1 (*Abstract Syntax Notation One*). Esta linguagem também especifica a forma pela qual os dados são representados, sendo independente da plataforma.
- **Codificação** - Cada objecto é codificado/descodificado usando a codificação BER (*Basic Encoding Rules*), permitindo a correcta transmissão dos objectos entre sistemas baseados na mesma arquitectura ou até mesmo em arquitecturas diferentes.

3.1.2.1 Nomes dos Objectos

Os objectos de gestão são organizados hierarquicamente numa árvore de objectos. Um objecto é identificado pelo seu OID, sendo este constituído por um conjunto de números separados por pontos. O OID também pode ser representado numa forma mais legível constituída por palavras separadas por pontos.

A partir da raiz da árvore são definidos três nós: `ccitt(0)`, `iso(1)` e `joint-iso-ccitt(2)`. O primeiro para objectos geridos pela CCITT (*International Telegraph and Telephone Consultative Committee*), actualmente ITU (*International Telecommunication Union*). O segundo para objectos geridos pela ISO (*International Organization for Standardization*) e o terceiro para objectos geridos conjuntamente pela CCITT e pela ISO.

No protocolo SNMP apenas o ramo `iso(1)` é usado. Sob este ramo a ISO definiu um ramo para organizações, o `org(3)`. Uma das organizações designadas pela ISO para a gestão de objectos foi o Departamento de Defesa dos Estados Unidos da América (DoD), com o ramo `dod(6)`. Sob este nó foi definido o ramo `internet(1)`.

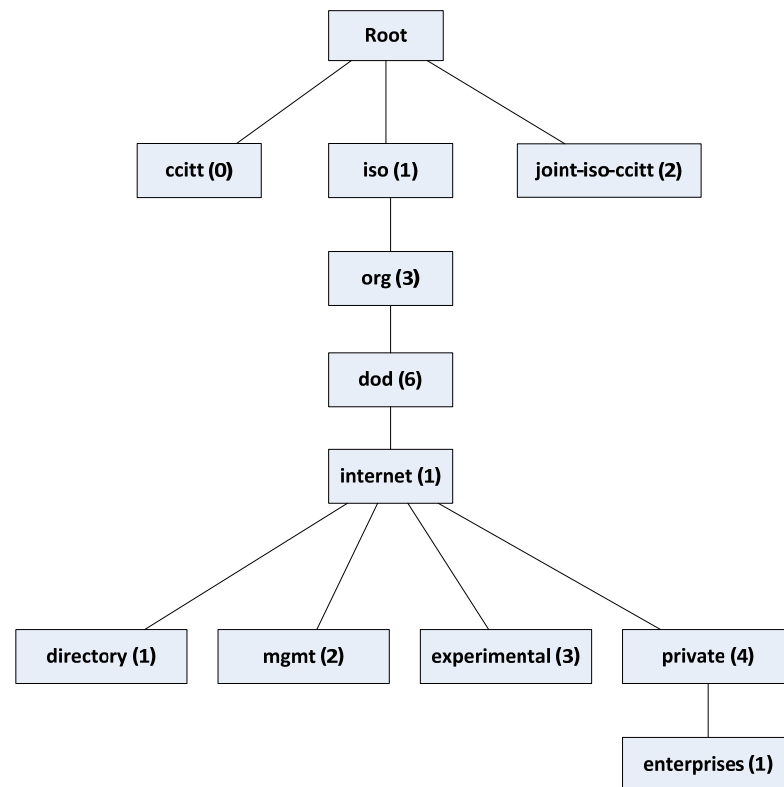


Figura 3.2 - Árvore de objectos definidos na SMIv1

O ramo `internet (1)`, gerido pela IANA (*Internet Assigned Numbers Authority*) tem o seguinte identificador:

```
internet          OBJECT IDENTIFIER ::= { iso 3 6 1 }
```

Sob este ramo foram definidos os quatro seguintes nós:

```
directory          OBJECT IDENTIFIER ::= { internet 1 }
mgmt                OBJECT IDENTIFIER ::= { internet 2 }
experimental        OBJECT IDENTIFIER ::= { internet 3 }
private             OBJECT IDENTIFIER ::= { internet 4 }
```

O nó `directory (1)` actualmente não é utilizado. Foi criado para uma futura ligação ao sistema de directório do modelo OSI.

O nó `mgmt (2)` foi criado para incluir os objectos de gestão da internet. Sob este nó encontra-se a *MIB Standard* da Internet.

O nó `experimental (3)`, tal como o próprio nome sugere, é utilizado para teste e desenvolvimento.

O nó `private(4)` contém apenas o seguinte ramo:

```
enterprises          OBJECT IDENTIFIER ::= { private 1 }
```

Este ramo foi criado para dar a oportunidade aos fabricantes de *software* e *hardware* de poderem definir os seus próprios objectos. Esta possibilidade é um trunfo do protocolo SNMP, pois permite o crescimento do número de objectos de uma forma organizada. Cada fabricante tem liberdade para organizar os objectos do seu ramo da forma que entender.

Na figura seguinte é possível observar alguns dos ramos existentes sob o nó `enterprises(1)`.

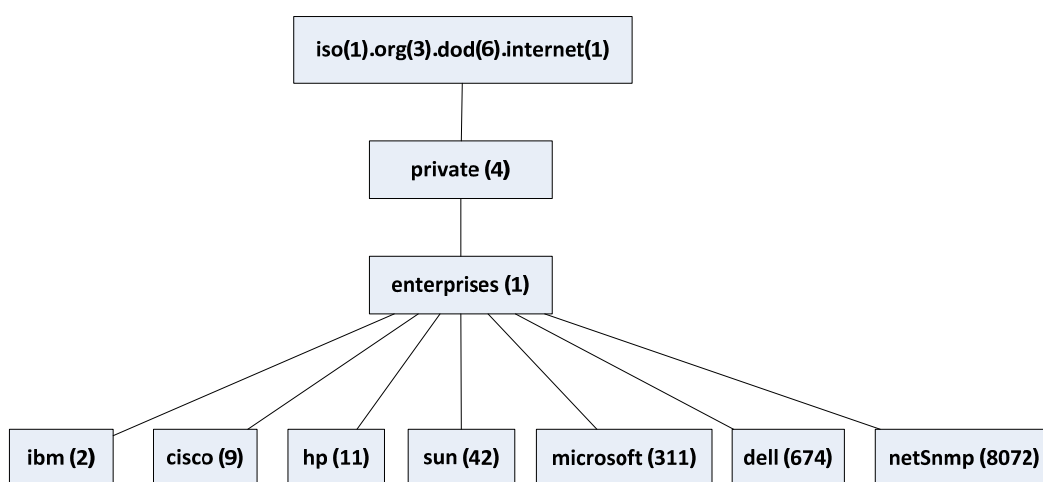


Figura 3.3 - Árvore com o ramo enterprises

A atribuição de números no ramo `enterprises(1)` é feita pela IANA, podendo ser atribuídos a indivíduos, instituições, organizações, empresas, etc.

3.1.2.2 Sintaxe dos Objectos

A sintaxe é utilizada para definir a estrutura de dados de cada objecto. É utilizado um subconjunto da linguagem ASN.1.

Tipos de dados primitivos utilizados no protocolo SNMP da linguagem ASN.1:

- `INTEGER` - Representa um número inteiro de 32bit com sinal, originando uma intervalo de representação entre -2^{31} (-2.147.483.648) e $2^{31} - 1$ (2.147.483.647). É normalmente usado para especificar tipos enumerados.
- `OCTET STRING` - Uma *string* de zero ou mais octetos, normalmente utilizada para representar sequências de caracteres. Nalguns casos também pode ser utilizada para representar endereços físicos.
- `OBJECT IDENTIFIER` - Uma *string* separada por pontos representando um objecto na árvore de gestão. Por exemplo, a *string* 1.3.6.1.2 representa o OID do ramo de gestão da internet (iso.org.dod.internet.mgmt).
- `NULL` - Não é usado no protocolo SNMP.

São também permitidos os seguintes tipos complexos (*Constructor Types*) que permitem a construção de listas e tabelas:

- `SEQUENCE` - Define uma lista de outros tipos de dados ASN.1.
- `SEQUENCE OF` - Define um objecto composto por um conjunto de elementos do tipo `SEQUENCE`. Normalmente utilizado para a construção de tabelas.

Na primeira versão da SMI (SMIv1) foram definidos os seguintes tipos de dados (*Defined Types*):

- `Counter` - Representa um número inteiro de 32bit sem sinal, originado um intervalo de representação entre 0 e $2^{32} - 1$ (4.294.967.295). Quando o valor máximo é atingido volta novamente a zero. O seu valor é sempre crescente, excepto quando o agente é reiniciado onde o seu valor inicial deverá ser zero. É normalmente utilizado para monitorizar a informação do número de pacotes ou octetos de um determinado interface de rede.
- `IpAddress` - Usado para representar endereços de rede IPv4.
- `NetworkAddress` - Do tipo do anterior mas utilizado para representar endereços de rede de outras famílias de endereços.
- `Gauge` - Representa um número inteiro de 32bit sem sinal. Ao contrário do tipo `Counter`, o valor deste pode aumentar ou diminuir ao longo do tempo.

- **TimeTicks** - Representa um número inteiro de 32bit utilizado para medir tempo em centésimos de segundo.
- **Opaque** - Permite armazenar qualquer outro tipo ASN.1 numa OCTET STRING.

A linguagem ASN.1 possui a possibilidade de criar Macros, permitindo uma extensão da própria linguagem. A SMIv1 possui a macro **OBJECT-TYPE** que permite definir um objecto gerido:

```
OBJECT-TYPE MACRO ::=
BEGIN
    TYPE NOTATION ::= "SYNTAX" type (TYPE ObjectSyntax)
                        "ACCESS" Access
                        "STATUS" Status
    VALUE NOTATION ::= value (VALUE ObjectName)

    Access ::=
        "read-only"
        | "read-write"
        | "write-only"
        | "not-accessible"
    Status ::=
        "mandatory"
        | "optional"
        | "obsolete"
END
```

Para definir um objecto usando a Macro **OBJECT-TYPE** é utilizada a seguinte sintaxe:

```
<Nome do Objecto> OBJECT-TYPE
    SYNTAX <Tipo de dados>
    ACCESS <read-only, read-write, write-only, not-accessible>
    STATUS <mandatory, optional, obsolete>
    DESCRIPTION
        "Descrição textual do objecto em causa."
    ::= { <OID Identificador do Objecto> }
```

Por exemplo, o objecto que contém a contagem de tempo desde que o agente de gestão de um sistema foi inicializado (`sysUpTime`) é definido da seguinte forma:

```
sysUpTime OBJECT-TYPE
    SYNTAX      TimeTicks
    ACCESS      read-only
    STATUS      mandatory
    DESCRIPTION
        "The time (in hundredths of a second) since the
        network management portion of the system was last
        re-initialized."
    ::= { system 3 }
```

3.1.2.2.1 SMIv2

A segunda geração do protocolo SNMP (SNMPv2) levou ao aparecimento de uma segunda versão da SMI, a SMIv2 [8]. Esta nova versão da SMI não substitui a anterior, apenas a expande, isto é, inclui todas as funcionalidades existentes e acrescenta mais algumas.

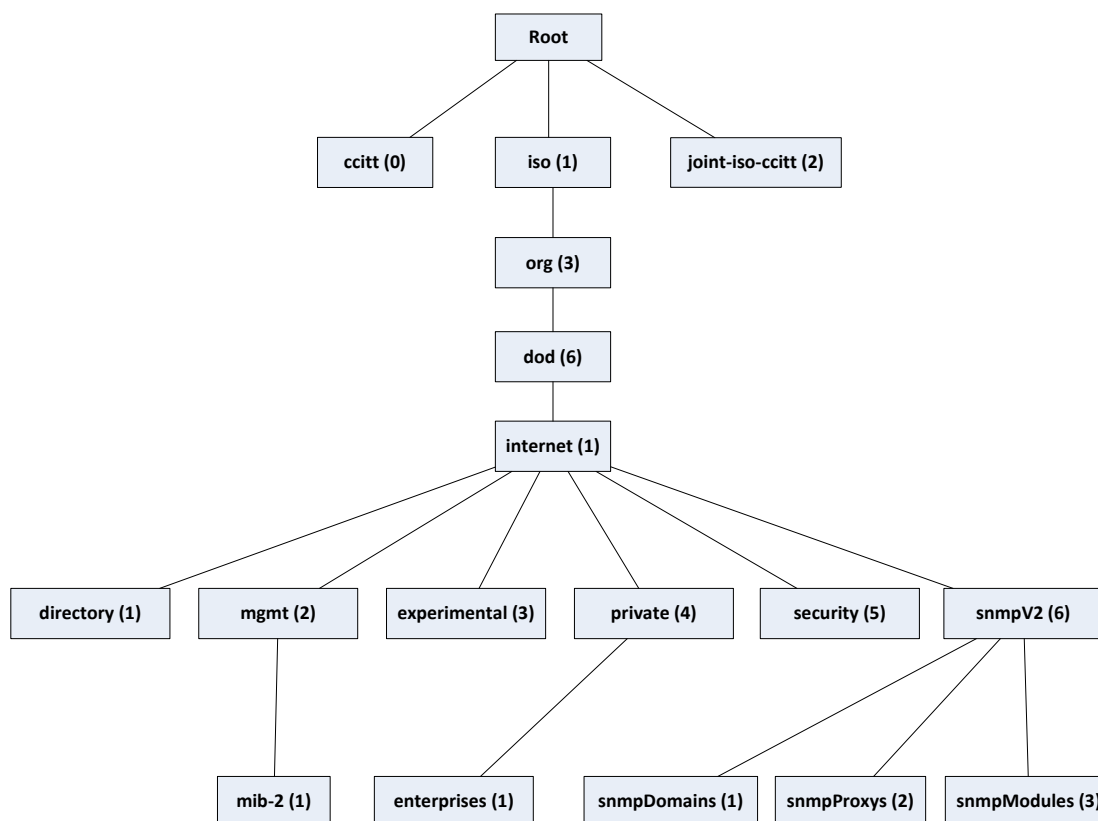


Figura 3.4 - Árvore de objectos definidos na SMIv2

Na SMIv2 são também definidos os seguintes novos tipos de dados:

- `Integer32` - Equivalente ao tipo `INTEGER` existente na SMIv1.
- `Counter32` - Equivalente ao tipo `Counter` existente na SMIv1.
- `Gauge32` - Equivalente ao tipo `Gauge` existente na SMIv1.
- `Unsigned32` - Representa um valor inteiro de 32bit sem sinal, originando um intervalo de representação entre 0 e $2^{32} - 1$ (4.294.967.295).
- `Counter64` - Semelhante ao tipo `Counter`, mas com um intervalo de representação de 0 a $2^{64} - 1$ (18.446.744.073.709.551.615). É útil para situações onde um objecto do tipo `Counter` chega em pouco tempo ao seu valor máximo. Por exemplo num interface *Gigabit Ethernet*

com uma grande ocupação da sua largura de banda um objecto do tipo `Counter` chega rapidamente ao seu valor máximo em menos de 5 minutos.

- `BITS` - Enumeração de *named bits*.

A macro `OBJECT-TYPE`, existente na SMIv1 foi alterada. Com a nova macro é permitido um melhor controlo da forma como o objecto é acedido, é dada a possibilidade de adicionar uma descrição textual das unidades usadas para representar o objecto e permite estender uma tabela adicionando uma ou mais colunas. Para declarar um objecto usando esta macro é utilizada a seguinte sintaxe:

```
<Nome do Objecto> OBJECT-TYPE
    SYNTAX <Tipo de dados>
    UnitsParts <Descrição textual das unidades usadas>
    MAX-ACCESS <read-only, read-write, read-create, not-accessible,
accessible-for-notify>
    STATUS <current, obsolete, deprecated>
    DESCRIPTION
        "Descrição textual do objecto em causa."
    AUGMENTS { <Nome da Tabela> }
    ::= { <OID Identificador do Objecto> }
```

São também introduzidas convenções textuais que permitem criar objectos de forma mais abstracta. As convenções textuais definidas na SMIv2 são as seguintes:

- `DisplayString` - Informação textual do conjunto de caracteres NVT (*Network Virtual Terminal*) ASCII.
- `PhysAddress` - Endereço físico representado como uma `OCTET STRING`.
- `MacAddress` - Endereço MAC, representado com seis octetos.
- `TruthValue` - Valor booleano.
- `TestAndIncr` - Usado para evitar que duas estações de gestão modifiquem o mesmo objecto ao mesmo tempo.
- `AutonomousType` - OID usado para definir uma sub-árvore adicional.
- `VariablePointer` - Apontador para um objecto.

- `RowPointer` - Apontador para uma linha de uma tabela.
- `RowStatus` - Usado para adicionar ou apagar linhas numa tabela.
- `TimeStamp` - Valor do objecto `sysUpTime` numa ocorrência.
- `TimeInterval` - Intervalo de tempo em centésimos de segundo. Poderá ter um valor máximo de 2.147.483.647.
- `DateAndTime` - Data e hora numa `OCTET STRING`.
- `StorageType` - Define o tipo de memória utilizado no agente.
- `TDomain` - Tipo de serviço de transporte.
- `TAddress` - Endereço do serviço de transporte.

3.1.2.2.2 MIB-II

A MIB-II [9] é uma evolução da MIB-I, sendo a MIB mais importante encontrada no SNMP, não só pela obrigatoriedade de ser suportada pelos equipamentos que implementam o protocolo SNMP, mas também pela informação que é possível retirar dos objectos que lá se encontram.

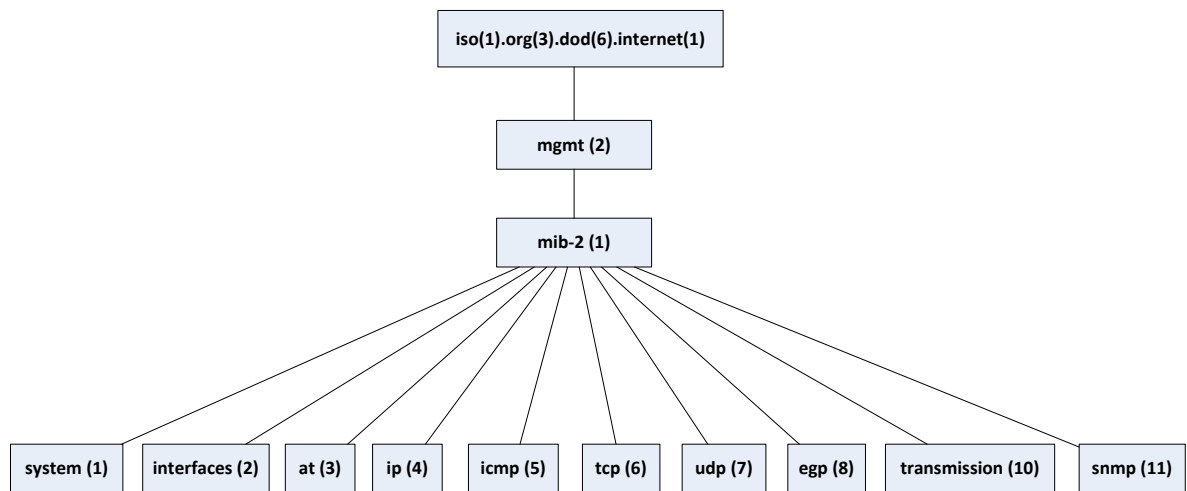


Figura 3.5 - Árvore com os principais objectos da MIB-II

- `system(1)` - É definido uma lista de objectos pertencentes à operação do sistema, tais como nome do sistema (`sysName`) e contacto (`sysContact`).
- `interfaces(2)` - Mantém informação de cada interface de rede de um sistema gerido. É possível encontrar informações tais como estado do interface, velocidade, número de pacotes recebidos e enviados e número de octetos enviados e recebidos.
- `at(3)` - Este grupo (*Address Translation*) contém uma tabela onde é possível fazer a tradução entre endereço de rede e endereço físico. É apenas mantido para manter a compatibilidade com a MIB-I, não devendo ser usado.
- `ip(4)` - Contém informação estatística de pacotes IP, assim como a tabela de encaminhamento do equipamento gerido.
- `icmp(5)` - Contém informação estatística sobre os pacotes ICMP (*Internet Control Message Protocol*).
- `tcp(6)` - Contém informação estatística sobre pacotes TCP e uma tabela com o estado das ligações TCP.

- `udp(7)` - Contém informação estatística sobre pacotes UDP e uma tabela que contém os portos UDP onde o equipamento gerido está à escuta.
- `egp(8)` - Contém informação estatística sobre o protocolo EGP assim como uma tabela com os vários vizinhos EGP.
- `transmission(10)` - Não são definidos objectos para este grupo na MIB-II. O objectivo deste grupo é servir de raiz para outras MIBs com objectos específicos para cada tipo de interface de rede.
- `snmp(11)` - Contém informação estatística sobre o sistema SNMP presente no agente.

3.1.3 Protocolo de Gestão

O Protocolo de Gestão é utilizado para a transferência de informação entre as entidades intervenientes no protocolo SNMP. Este protocolo está situado ao nível de aplicação do modelo de camadas TCP/IP, usando o protocolo UDP para transporte. A escolha de um protocolo de transporte não fiável, como o protocolo UDP, deve-se ao menor *overhead* introduzido pelo próprio protocolo de transporte, visto que a introdução de um sistema de gestão numa rede deverá provocar o mínimo de impacto sobre essa rede. O problema da não garantia de entrega ao nível da camada de transporte é facilmente contornado pela implementação de um simples mecanismo de *timeout* ao nível da camada de aplicação. Só poderá haver um problema maior na entrega de notificações à estação de gestão, visto que as notificações não são confirmadas.

O porto UDP definido para os agentes foi o 161 e o das estações de gestão de forma a receberem as notificações o 162.

Os protocolos SNMPv1 e SNMPv2 baseiam-se na noção de comunidade para estabelecer autenticação entre as estações de gestão e os agentes. O agente é configurado com três nomes de comunidade (*community strings*). Um que permite o acesso aos objectos agente apenas para operações de leitura (*read-only*), outro que permite o acesso de leitura e escrita aos objectos do agente (*read-write*) e finalmente um usado pelos agentes para enviarem notificações às estações de gestão (*trap*). Na prática estes nomes de comunidade são basicamente *passwords*.

A seguir é apresentado o PDU (*Protocol Data Unit*) de uma mensagem SNMP, ou seja os dados que são transportados pela camada de transporte do protocolo de comunicação.

Version	Community	SNMP PDU
---------	-----------	----------

Figura 3.6 - PDU de uma mensagem SNMP

- Version
 - 0 - SNMPv1
 - 1 - SNMPv2
- Community - *community string*

3.1.3.1 SNMPv1

A primeira versão do protocolo definiu as seguintes operações:

- GetRequest (0)
- GetNextRequest (1)
- GetResponse (2)
- SetRequest (3)
- Trap (4)

Em todos os PDUs existe o campo *Variable Bindings* que é composto por um ou mais conjuntos de OID e valor, tal como é ilustrado na figura seguinte.

OID ₁	Value ₁	OID ₂	Value ₂	...	OID _n	Value _n
------------------	--------------------	------------------	--------------------	-----	------------------	--------------------

Figura 3.7 - Variable Bindings presente nos PDUs SNMP

3.1.3.1.1 GetRequest, GetNextRequest e SetRequest

A operação *GetRequest* é utilizada pelas estações de gestão com o objectivo de requisitarem informação aos agentes. Poderão requisitar mais do que um objecto na mesma mensagem. O campo *PDU-Type*, para esta operação, é preenchido com o valor 0.

A operação *GetNextRequest*, tal como a anterior, é utilizada pelas estações de gestão com a finalidade de obterem o OID e valor do objecto seguinte.

O campo *PDU-Type*, para esta operação, é preenchido com o valor 1.

A operação *SetRequest* permite às estações de gestão alterarem valores de objectos nos agentes. O campo *PDU-Type*, para esta operação, deverá ser preenchido com o valor 3.

Qualquer uma das operações *GetRequest*, *GetNextRequest* ou *SetRequest* usa o mesmo formato de mensagem tal como é visível na figura seguinte. A resposta a qualquer uma destas operações é realizada pelos agentes usando a operação *GetResponse*.

PDU Type	Request-ID	0	0	Variable Bindings
----------	------------	---	---	-------------------

Figura 3.8 - PDU SNMPv1 das operações *GetRequest*, *GetNextRequest* e *SetRequest*

3.1.3.1.2 GetResponse

Esta operação é utilizada pelo agente para responder aos pedidos `GetRequest` e `GetNextRequest` assim como efectuar a confirmação à operação `SetRequest`. O PDU definido nas especificações do SNMPv1 para esta operação é apresentado a seguir.

PDU Type	Request-ID	Error-Status	Error-Index	Variable Bindings
----------	------------	--------------	-------------	-------------------

Figura 3.9 - PDU SNMPv1 da operação GetResponse

O campo `PDU Type` é preenchido com o valor 2, sendo o campo `Request-ID` preenchido com o mesmo valor do campo `Request-ID` da pergunta, de forma a que a estação de gestão possa relacionar a pergunta com a resposta.

No PDU da operação `GetResponse` está presente o campo `Error-Status` que dá a indicação de algum eventual problema ao gerar a resposta. Caso o valor deste campo seja diferente de zero, ou seja uma situação de erro, o campo `Error-Index` aponta para o objecto que deu origem ao erro.

O campo `Error-Status` pode tomar um dos seguintes valores:

- `noError(0)` - Não ocorreu nenhum problema.
- `tooBig(1)` - A resposta ao pedido é demasiado grande.
- `noSuchName(2)` - Foi pedido um valor ou foi pedida a alteração de um objecto que não existe.
- `badValue(3)` - O valor do objecto não é consistente.
- `readOnly(4)` - Geralmente não é utilizado. O erro `noSuchName(2)` é equivalente.
- `genErr(5)` - Erro genérico utilizado quando nenhum dos anteriores se aplica.

3.1.3.1.3 Trap

A operação Trap é realizada pelos agentes presentes nos equipamentos geridos, enviando para a estação de gestão informação de ocorrências importantes. O PDU definido nas especificações do SNMPv1 para esta operação é apresentado a seguir.

PDU Type	Enterprise	Agent-Addr	Generic-Trap	Specific-Trap	Time-Stamp	Variable Bindings
----------	------------	------------	--------------	---------------	------------	-------------------

Figura 3.10 - PDU SNMPv1 da operação Trap

- **PDU Type** - Toma o valor 4 (Trap).
- **Enterprise** - Contém o OID que identifica o equipamento. Normalmente é utilizado o valor do objecto `sysObjectID`.
- **Agent-Addr** - Endereço do agente que gerou o trap.
- **Time-Stamp** - Indica o intervalo de tempo desde que o agente foi inicializado e o momento em que foi gerado o trap. Normalmente é o valor do objecto `sysUpTime`.

O campo **Generic-Trap** poderá tomar um dos seguintes valores:

- `coldStart(0)` - Indica que o agente foi reiniciado. Todos os objectos de gestão serão inicializados. Os contadores irão tomar o valor zero.
- `warmStart(1)` - Indica que o agente reiniciou e nenhum dos objectos de gestão será inicializado.
- `linkDown(2)` - Indica que um interface de rede passou para o estado inactivo.
- `linkUp(3)` - Indica que um interface de rede passou para o estado activo.
- `authenticationFailure(4)` - Dá a indicação que houve uma falha de autenticação na *community string*.
- `egpNeighborLoss(5)` - Indica que houve uma perda de um vizinho do protocolo EGP (Exterior Gateway Protocol).
- `enterpriseSpecific(6)` - Dá a indicação que o trap é específico de uma MIB privada, indicando no campo **Specific-Trap** o OID do objecto dessa MIB.

3.1.3.2 SNMPv2

A segunda versão do protocolo SNMP (SNMPv2) com os objectivos de permitir a transferência de grandes quantidades de informação, comunicação entre estações de gestão e normalização das mensagens de notificação, introduziu as seguintes novas operações:

- GetBulkRequest (5)
- InformRequest (6)
- SNMPv2-Trap (7)
- Report (8)

A operação Trap foi tornada obsoleta, visto que esta versão introduz a operação SNMPv2-Trap. As restantes operações existentes no SNMPv1 são suportadas nesta versão, não tendo sido alterado o seu formato.

3.1.3.2.1 GetBulkRequest

O objectivo desta operação foi permitir pedidos de transferência de grandes quantidades de informação, como por exemplo a transferência de tabelas. Na anterior versão também era possível transferir grandes quantidades de informação, mas essa transferência era efectuada à custa de uma grande quantidade de pedidos do tipo GetNextRequest. O campo `PDU Type` é preenchido com o valor 5.

PDU Type	Request-ID	Non-Repeaters	Max-Repetitions	Variable Bindings
----------	------------	---------------	-----------------	-------------------

Figura 3.11 - PDU SNMPv2 da operação GetBulkRequest

3.1.3.2.2 InformRequest

A operação InformRequest foi introduzida de forma a permitir a comunicação entre estações de gestão, tendo o mesmo formato das operações GetRequest, GetNextRequest e SetRequest. O campo `PDU Type` é preenchido com o valor 6.

PDU Type	Request-ID	0	0	Variable Bindings
----------	------------	---	---	-------------------

Figura 3.12 - PDU SNMPv2 da operação InformRequest

3.1.3.2.3 SNMPv2-Trap

Esta operação é semelhante à operação Trap, existente no SNMPv1. A principal diferença reside no PDU. Passa a ter o formato dos PDUs das operações GetRequest, GetNextRequest, SetRequest e InformRequest, sendo a razão da notificação dada no campo `Variable Bindings` através de objectos do tipo NOTIFICATION-TYPE. O campo `PDU-Type`, para esta operação, deverá ser preenchido com o valor 7.

PDU Type	Request-ID	0	0	Variable Bindings
-----------------	-------------------	----------	----------	--------------------------

Figura 3.13 - PDU SNMPv2 da operação SNMPv2-Trap

3.1.3.2.4 Report

Esta operação foi prevista no RFC, mas nunca foi implementada.

Devido à falta de robustez nas mensagens de erro da anterior versão do protocolo foram introduzidas as seguintes novas mensagens de erro em resposta às operações GetRequest, GetNextRequest, GetBulkRequest e SetRequest:

- `noAccess(6)` - Este erro é normalmente gerado quando é realizada uma tentativa de alteração do valor de um objecto inacessível.
- `wrongType(7)` - O valor do objecto não é consistente com o seu tipo.
- `wrongLenght(8)` - O valor do objecto não tem o tamanho especificado.
- `wrongEncoding(9)` - A codificação do valor do objecto não está correcta.
- `wrongValue(10)` - O valor do objecto não está correcto.
- `noCreation(11)` - O objecto não existe na MIB.
- `inconsistentValue(12)` - O objecto está num estado inconsistente, não permitindo a alteração do seu valor.
- `resourceUnavailable(13)` - Não existem recursos suficientes para que seja possível a alteração do valor de um objecto.
- `commitFailed(14)` - Erro genérico para as operações de alteração do valor de um objecto. Utilizado para quando nenhum dos outros erros é aplicável.
- `undoFailed(15)` - A operação de alteração de um valor falhou e o agente não conseguiu desfazer todas as alterações que já tinha efectuado.
- `authorizationError(16)` - A *community string* não está correcta.

- `notWritable(17)` - O objecto não permite a alteração do valor.
- `inconsistentName(18)` - O objecto não existe, nem pode ser criado nessa situação.

Outra diferença introduzida foi a capacidade de transporte dos PDUs em múltiplos protocolos de transporte. Para além do protocolo de transporte suportado na versão anterior, o protocolo UDP, foi também definido o suporte dos seguintes protocolos de transporte:

- *OSI Connectionless-Mode Network Service (CLNS)*
- *OSI Connection-Oriented Network Service (CONS)*
- *AppleTalk Datagram Delivery Protocol (DDP)*
- *Novell Internetwork Packet Exchange (IPX)*

3.1.3.3 SNMPv3

A terceira geração do protocolo SNMP (SNMPv3) não introduz nenhuma alteração ao protocolo, mantendo as mesmas operações existentes no SNMPv2. O principal objectivo desta nova versão foi a resolução do problema da segurança.

Outra das grandes diferenças é o abandono da noção de estação de gestão e agentes, sendo ambos chamados entidades SNMP (*SNMP Entity*). Cada entidade SNMP é composta por um motor SNMP (*SNMP Engine*) e por uma ou mais aplicações SNMP (*SNMP Applications*).

A figura seguinte ilustra a arquitectura definida na terceira versão do protocolo SNMP.

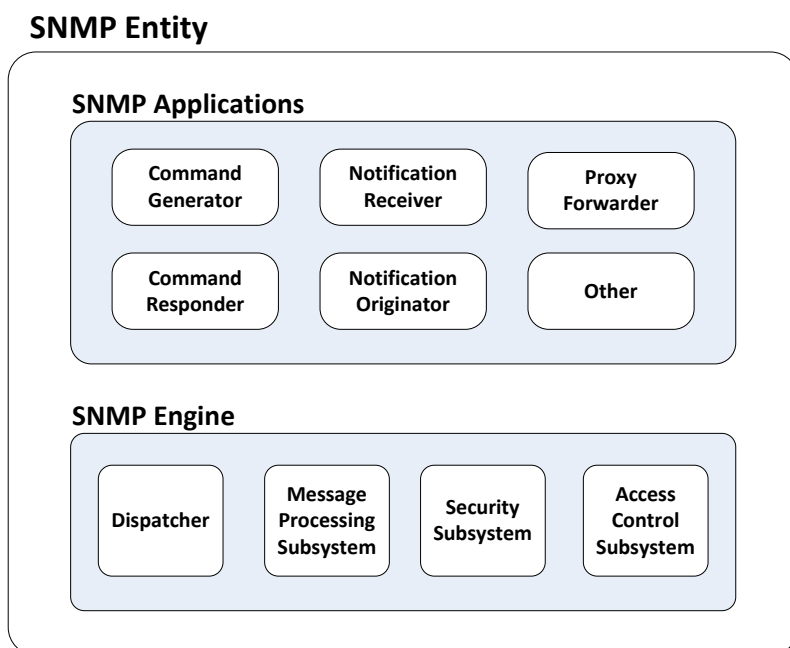


Figura 3.14 - Arquitectura SNMPv3

O motor SNMP é responsável por enviar, receber, autenticar e encriptar mensagens, assim como controlar o acesso aos objectos geridos. As suas componentes são as seguintes:

- **Dispatcher** - Subsistema responsável por receber e enviar as mensagens para o respectivo modelo do subsistema de processamento de mensagens.
- **Message Processing Subsystem** - Responsável por preparar as mensagens para enviar ou extrair os dados das mensagens recebidas, tendo a capacidade de suportar mensagens em qualquer versão do protocolo SNMP.
- **Security Subsystem** - Subsistema responsável por autenticar e encriptar ou desencriptar mensagens.
- **Access Control Subsystem** - Subsistema responsável por controlar o acesso aos objectos geridos, assim como determinar quais as operações que são permitidas realizar sobre esses objectos.

As aplicações SNMP utilizam os serviços fornecidos pelo motor SNMP para realizarem as suas operações. Existem os seguintes tipos de aplicações:

- ***Command Generator*** - Responsável por gerar os pedidos e processar as respostas.
- ***Command Responder*** - Responsável pelo acesso à informação de gestão.
- ***Notification Originator*** - Gera mensagens de notificação.
- ***Notification Receiver*** - Recebe as mensagens de notificação.
- ***Proxy Forwarder*** - Encaminha as mensagens entre entidades.

Tipicamente uma estação de gestão terá que conter as seguintes aplicações:

- ***Command Generator***
- ***Notification Receiver***

Um agente num equipamento gerido terá que conter as seguintes aplicações:

- ***Command Responder***
- ***Notification Originator***

3.2 Gestão de Redes

A Gestão de Redes de uma forma generalizada consiste na utilização de várias ferramentas, técnicas e sistemas de forma a garantir o bom funcionamento de uma rede, realizando uma gestão eficiente dos recursos e equipamentos.

De forma a organizar os requisitos de gestão de redes a Organização Internacional para a Normalização (ISO) definiu as seguintes áreas funcionais [10]:

- Gestão de Falhas
- Gestão da Contabilização
- Gestão da Configuração
- Gestão do Desempenho
- Gestão da Segurança

Embora esta classificação tenha sido inicialmente desenvolvida para o modelo de gestão de redes OSI (*Open Systems Interconnection*) tem ganho aceitação pela maioria dos outros sistemas devido à sua forma eficaz de organização dos requisitos.

3.2.1 Áreas Funcionais

3.2.1.1 Gestão de Falhas

O objectivo desta área funcional é garantir o bom funcionamento de uma infra-estrutura de rede, sendo necessário garantir que cada componente constituinte da rede esteja em boas condições de funcionamento. Deste modo quando ocorre uma falha é importante:

- Determinar o ponto onde ocorreu a falha.
- Isolar o resto da rede da falha de modo a que seja possível o seu correcto funcionamento sem interferência do ponto onde ocorreu a falha.
- Reconfigurar a rede de modo a minimizar o impacto da operação sem o(s) equipamento(s) defeituoso(s).
- Reparar ou substituir o(s) equipamento(s) defeituoso(s) de forma a repor o estado original da rede.

Um conceito fundamental para a gestão de falhas é a própria definição de falha. Uma falha é diferente de um erro. É uma condição anormal que requer atenção e/ou intervenção, enquanto um erro é apenas um evento isolado. No entanto uma falha pode ser indicada por erros excessivos.

3.2.1.2 Gestão da Contabilização

O objectivo desta área funcional é contabilizar a utilização dos recursos da rede associados a cada utilizador ou grupos de utilizadores. Desta forma é possível a detecção de gastos excessivos de utilizadores que limitam a utilização da rede, assim como a detecção de utilizações ineficientes de determinados recursos.

A informação obtida nesta área permite desenvolver um plano de crescimento da infra-estrutura.

Nos casos onde existe necessidade de taxaço pela utilização dos recursos da rede, as informações de consumos são obtidas nesta área.

3.2.1.3 Gestão da Configuração

A área de gestão da configuração tem como responsabilidade obter, documentar e armazenar os parâmetros mais adequados ao bom funcionamento de uma infra-estrutura de rede, assim como garantir a configuração de cada equipamento que constitui a rede.

Em infra-estruturas de rede com alguma dimensão e grande número de equipamentos torna-se importante a existência de processos automatizados para alteração da configuração ou actualização de software dos equipamentos.

3.2.1.4 Gestão do Desempenho

Esta área funcional é responsável pela monitorização e controlo da rede com o objectivo de manter ou melhorar o desempenho de uma infra-estrutura de rede.

A monitorização consiste na recolha de informação e posterior comparação dessa informação com indicadores de condições normais e desejáveis de funcionamento.

O controlo corresponde às acções tomadas no sentido da melhoria do desempenho da rede, com base na informação recolhida na monitorização.

O desempenho da rede pode ser afectado por problemas noutras áreas de gestão, mas em condições normais de funcionamento pode ser medido por alguns dos seguintes indicadores:

- Taxa de utilização
- Tempo de resposta
- Taxa de erros

Em infra-estruturas de redes sem fios existem indicadores adicionais tais como:

- Relação sinal ruído (SNR) da ligação rádio
- Número de utilizadores associados aos pontos de acesso

3.2.1.5 Gestão da Segurança

A gestão da segurança é responsável pela protecção da informação e pelo controlo de acesso aos recursos disponibilizados por uma rede. Além disto, também é responsável pelo registo dos acessos aos recursos e informação.

A gestão da segurança em redes Wi-Fi tem um papel mais importante devido à natureza do canal de comunicação. A utilização de mecanismos de autenticação e encriptação no canal rádio torna-se obrigatório de forma a garantir a confidencialidade das comunicações.

3.2.2 Soluções existentes

A área de gestão de redes é uma área bastante rica em plataformas de monitorização e gestão, mas a maioria das plataformas não foram concebidas para gerir redes Wi-Fi, ou seja não resolvem os problemas de gestão inerentes a este tipo de redes.

A maioria dos equipamentos fornece software de gestão próprio, mas este tipo de solução apresenta o inconveniente de ser específico para um determinado tipo de equipamento, sendo habitualmente diferente de fabricante para fabricante. Nesta situação uma rede com alguma dimensão e equipamentos de fabricantes diferentes torna a tarefa de gestão muito complicada.

Alguns fabricantes de *hardware* Wi-Fi também fornecem soluções de gestão bastante poderosas para este tipo de redes. Algumas dessas soluções são:

- *CiscoWorks Wireless LAN Solution Engine* [11]
- *ProximVision Network Management System* [12]
- *Motorola RF Management Software* [13]

O grande problema das soluções anteriores centra-se na insuficiente ou até mesmo inexistente capacidade de suportar equipamentos de fabricantes diferentes.

Existem outras soluções que apenas fornecem monitorização de qualquer valor que seja fornecido pelo equipamento tais como:

- *MRTG (Multi Router Traffic Grapher)* [14]
- *Cacti* [15]

Qualquer uma das anteriores soluções apenas se limitam a recolher informação dos vários equipamentos e gerar gráficos com os valores recolhidos. No caso do Cacti de uma forma opcional poderão ser definidos patamares de valores de forma a que quando algum dos valores recolhidos ultrapasse o patamar definido durante um certo intervalo de tempo seja gerado um alerta.

Mais recentemente apareceram soluções de gestão integradas dedicadas a infra-estruturas de rede sem fios tais como:

- **AirWave Management Platform [16]**

Esta solução é uma plataforma de gestão de redes Wi-Fi bastante completa, pois permite a gestão dos vários equipamentos através de um interface Web. Suporta um grande leque de fabricantes de equipamento, permitindo a sua configuração remota através do protocolo SNMP. Também possui alguma inteligência, realizando diagnósticos da rede e gerando alarmes na detecção de eventuais problemas.

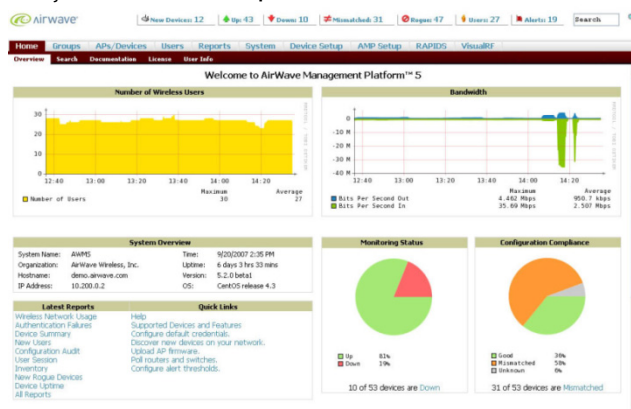


Figura 3.15 - Interface de gestão da plataforma AirWave Management Platform

- **ManageEngine WiFi Manager [17]**

Esta é uma solução que permite a gestão centralizada de redes Wi-Fi empresariais. Tem como características principais a monitorização e configuração de APs. Tal como a solução anterior utiliza um interface Web. Permite detectar ataques, tentativas de acesso à rede não autorizadas e eventuais vulnerabilidades da rede através de sondas Wi-Fi colocadas na rede. Segue-se uma captura do interface de gestão disponível para o gestor.

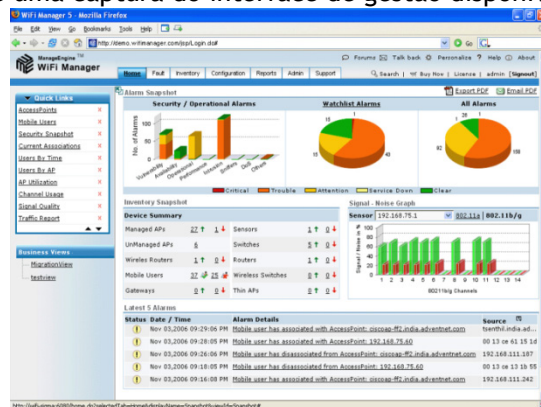


Figura 3.16 - Interface de gestão da plataforma ManageEngine WiFi Manager

A grande vantagem destas duas últimas soluções é a capacidade de suportarem equipamento de diferentes fabricantes, facilitando a sua integração numa rede já existente onde muito provavelmente existirão equipamentos de vários fabricantes.

Capítulo 4

Caracterização do Problema

Neste capítulo é efectuada a identificação dos requisitos da plataforma de gestão assim como uma análise a algumas MIBs relacionadas com a gestão de equipamentos com suporte da norma IEEE 802.11.

4.1 Identificação dos principais problemas de gestão e operação

A gestão de uma infra-estrutura de rede Wi-Fi origina inúmeros problemas. Serão seguidamente identificados e descritos alguns desses problemas, que deverão ser solucionados pela plataforma de gestão implementada.

4.1.1 Monitorização do Desempenho

A monitorização do desempenho permite detectar situações especiais que possam levar a um desempenho da rede inferior ao desejado. Permite também recolher informação para que sejam tomadas decisões de aumento de capacidade e/ou cobertura da rede. Segue-se uma lista com os principais indicadores que interessam recolher e guardar de forma a ter um histórico da evolução ao longo do tempo:

- Saber qual a ocupação, em termos de largura de banda, de todos os interfaces de rede dos equipamentos geridos (pontos de acesso, comutadores e routers) para que seja possível detectar situações de má qualidade de serviço devido à ocupação excessiva de um interface de rede.

- Determinar o número de utilizadores associados a cada ponto de acesso Wi-Fi, pois se este for elevado levará a uma degradação do serviço. No caso dos pontos de acesso que tenham mais do que um SSID é importante saber o número de estações por cada SSID.
- Determinar um indicador da qualidade de cobertura dos pontos de acesso, podendo este ser dado pela média do nível de sinal e/ou média da relação sinal/ruído recebida de todas as estações associadas a cada ponto de acesso.

4.1.2 Contabilização

De modo a controlar consumos excessivos ou nalguns casos aplicar uma taxação pelo consumo de tráfego, é importante determinar o volume de tráfego consumido por cada utilizador da rede.

4.1.3 Monitorização da Segurança

Sendo as redes em questão redes sem fios, estas são, por natureza, redes mais vulneráveis a tentativas de entrada não autorizadas, e como tal, os acessos à rede devem ser registados.

Também por vezes pode ser necessário identificar um utilizador pelo seu endereço IP ou endereço MAC utilizado num determinado momento, logo deverão existir registos que associem um utilizador ao endereço IP e endereço MAC do seu terminal.

4.1.4 Detecção de Falhas

Para a detecção de falhas, a monitorização de vários parâmetros dos equipamentos podem levar a que sejam detectadas situações de falha mesmo antes de estas acontecerem, daí também ser uma área importante para a minimização do tempo de indisponibilidade da rede.

Podem acontecer falhas na própria infra-estrutura cablada levando a taxas de erros elevadas nos interfaces *Ethernet* dos equipamentos activos.

O lado rádio da infra-estrutura pode também ser afectado por interferências de outros equipamentos que estejam próximos e a operar na mesma banda de frequências de algum ponto de acesso. Embora o protocolo de redes IEEE 802.11 tenha sido desenvolvido tomando em conta estas situações, tendo incluído mecanismos de verificação da integridade da trama

recebida e mecanismos de retransmissão de tramas, se o sinal interferente tiver uma potência bastante superior pode originar uma degradação elevada da ligação das estações móveis à rede, até à situação limite de impossibilidade de fornecimento do serviço de rede. Para resolver situações destas, os pontos de acesso mais recentes possuem uma funcionalidade que permite a escolha dinâmica do canal de operação, alterando-o de forma a operarem no canal menos sujeito a interferências. Possuir um histórico com registos do canal de operação ao longo do tempo pode ajudar a detectar situações destas caso existam saltos muito frequentes do canal de operação.

4.1.5 Configuração

A configuração remota dos equipamentos é um aspecto importante do sistema de gestão, pois permite poupar imenso tempo nas situações onde é necessário fazer alguma alteração na configuração de vários equipamentos em simultâneo. Em alguns casos existe o problema de os equipamentos serem de fabricantes diversos tendo cada um, métodos diferentes de configuração.

Nos pontos de acesso Wi-Fi as configurações mais habituais são a alteração de parâmetros associados ao(s) interface(s) rádio tais como:

- Canal de operação (pode também ser escolhida a atribuição dinâmica do canal pelo próprio ponto de acesso, caso possua esta funcionalidade).
- Potência de emissão (a diminuição da potência de emissão do ponto de acesso permite diminuir a interferência entre pontos de acesso próximos que operem nos mesmos canais ou canais adjacentes).
- Débitos máximos permitidos.

Também por vezes é necessário realizar alterações de parâmetros do SSID existente ou, caso o ponto de acesso permita, adicionar um ou mais SSIDs. Os parâmetros necessários para a sua configuração são:

- Nome do SSID
- Permitir ou não a difusão do SSID (*SSID Broadcast*)
- Escolha da VLAN associada, caso o ponto de acesso suporte VLANs

Os parâmetros relacionados com a segurança do SSID são:

- Modo de Autenticação (Aberto, Chave Partilhada ou EAP)
- Encriptação (Nenhum, WEP, TKIP ou AES)
- Chaves de autenticação e para encriptação de dados

Por questões de segurança da própria rede, por vezes é também necessário barrar o acesso à rede a determinados terminais pelo seu endereço MAC.

4.2 Análise das MIBs

4.2.1 MIB-II

A MIB-II é a MIB mais importante encontrada no protocolo SNMP. Alguns dos problemas podem ser resolvidos utilizando alguns dos objectos presentes desta MIB. A implementação de muitos objectos desta MIB nos agentes é obrigatória, levando a que não existam problemas ao obter a informação de equipamentos de diferentes fabricantes.

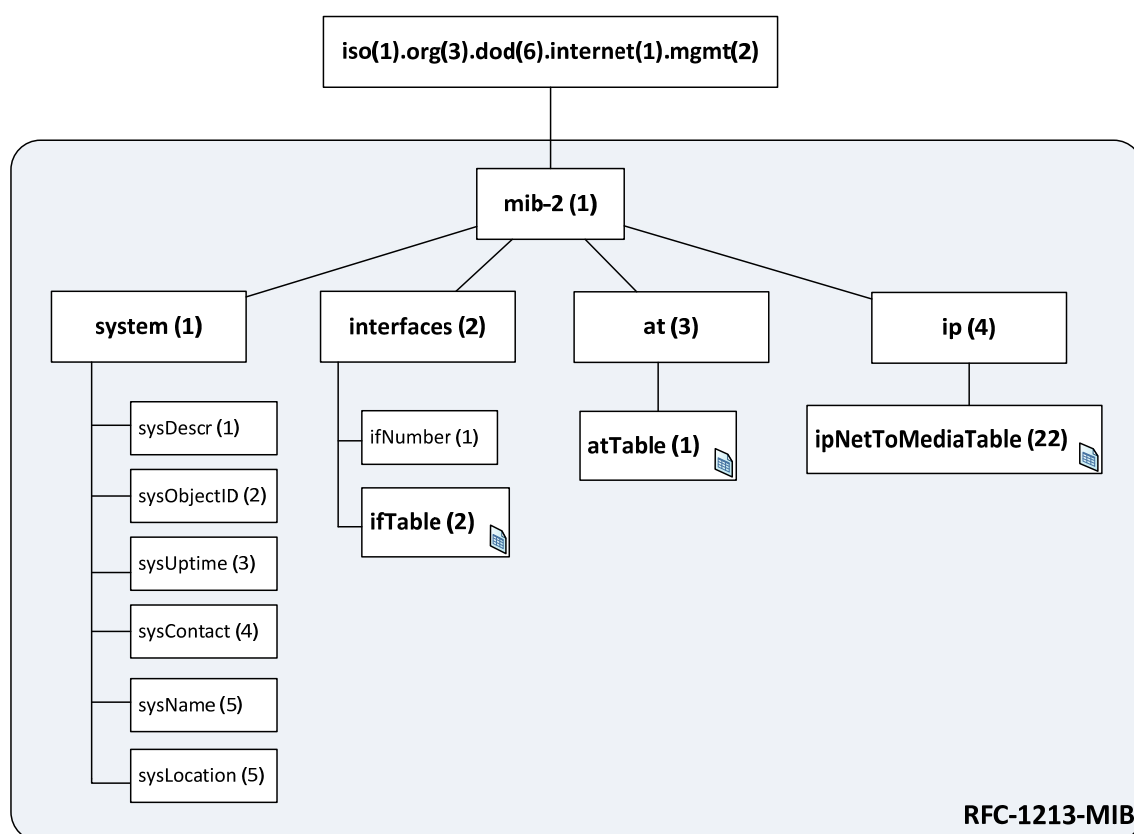


Figura 4.1 - Objectos importantes da MIB-II

O ramo `system` é composto por vários objectos que fornecem informação geral sobre o sistema gerido. É possível saber o fabricante, o modelo e versão de software através do objecto `sysDescr`.

O objecto `sysObjectID` apenas fornece um apontador para o objecto que identifica o sistema, normalmente dentro da MIB proprietária.

Outro objecto importante é o `sysUptime`. Este fornece a indicação do tempo desde que o agente SNMP foi reinicializado. É uma indicação importante pois permite saber se os vários contadores que existem na base de dados do agente foram reiniciados a 0, entre leituras consecutivas.

Os objectos `sysContact`, `sysName` e `sysLocation` são apenas informativos e até podem ser alterados pela estação de gestão.

O ramo `interfaces` é composto por informação genérica sobre os interfaces de rede do equipamento gerido. Sob este ramo estão presentes o objecto `ifNumber`, que indica o número de interfaces de rede que o sistema possui, e tabela `ifTable`.

Esta tabela possui uma entrada por cada interface de rede, sendo cada uma composta pelas seguintes colunas:

Tabela 4.1 - Tabela `ifTable` da MIB-II

ifTable (.1.3.6.1.2.1.2.2)		
ifEntry (1)	ifIndex (1)	Valor identificador do interface.
	ifDescr (2)	Descrição textual do interface.
	ifType (3)	Tipo de interface. Dos vários valores possíveis podem-se destacar os seguintes: ethernetCsmacd (6) - Ethernet ieee80211 (71) - 802.11
	ifMtu (4)	Tamanho máximo do pacote, em octetos, que pode ser enviado ou recebido pelo interface.
	ifSpeed (5)	Capacidade nominal do interface, em bits por segundo.
	ifPhysAddress (6)	Endereço físico do interface. Para a família IEEE802 é usado o endereço MAC do interface.
	ifAdminStatus (7)	Estado administrativo do interface. Pode ser alterado pela estação de gestão. Os valores possíveis são: Up (1) Down (2) Testing (3)
	ifOperStatus (8)	Estado operacional do interface. Os valores possíveis são: Up (1) Down (2) Testing (3)
	ifLastChange (9)	Valor do objecto <code>sysUptime</code> do momento em que o interface passou para o estado operacional actual.
	ifInOctets (10)	Contador do número de octetos recebidos pelo interface.
	ifInUcastPkts (11)	Contador do número de pacotes recebidos pelo interface com endereço de destino <i>unicast</i> .

	ifInNUcastPkts (12)	Contador do número de pacotes recebidos pelo interface com endereço de destino <i>broadcast</i> ou <i>multicast</i> .
	ifInDiscards (13)	Contador do número de pacotes recebidos pelo interface que foram descartados, mesmo não contendo erros.
	ifInErrors (14)	Contador do número de pacotes recebidos pelo interface com erros, não sendo entregues às camadas superiores.
	ifInUnknownProtos (15)	Contador do número de pacotes recebidos pelo interface que foram descartados devido ao protocolo não ser suportado pelo interface.
	ifOutOctets (16)	Contador do número de octetos enviados pelo interface.
	ifOutUcastPkts (17)	Contador do número de pacotes com endereço de destino unicast enviados pelo interface.
	ifOutNUcastPkts (18)	Contador do número de pacotes com endereço de destino <i>broadcast</i> ou <i>multicast</i> enviados pelo interface.
	ifOutDiscards (19)	Contador do número de pacotes descartados pelo interface, mesmo não contendo erros.
	ifOutErrors (20)	Contador do número de pacotes que não foram enviados pelo interface devido a erros.
	ifOutQLen (21)	Comprimento da fila de saída em número de pacotes.
	ifSpecific (22)	Referência à MIB que contenha objectos específicos deste interface.

O índice de cada entrada da tabela é o valor do campo `ifIndex`, sendo este um valor único para cada interface. Pode tomar valores entre 1 e o valor do objecto `ifNumber`. Este índice serve de referência a outras tabelas (até de outras MIBs) sempre que é necessário referenciar um interface de rede.

O ramo `at`, iniciais de *Address Translation*, é composto apenas pela tabela `atTable`. Esta tabela permite fazer o mapeamento entre um endereço de rede e o endereço físico de um interface de rede. Em LANs o endereço físico é o endereço MAC do interface de rede. O endereço de rede, no caso de redes IP, é o endereço IP.

Tabela 4.2 - Tabela atTable da MIB-II

atTable (.1.3.6.1.2.1.3.1)		
atEntry (1)	atIfIndex (1)	Valor identificador do interface onde o mapeamento se encontra activo.
	atPhysAddress (2)	Endereço físico. Normalmente o endereço MAC.
	atNetAddress (3)	Endereço de rede. Em redes IP é o endereço IP.

De forma a resolver o problema da existência de múltiplas entradas para o mesmo endereço físico, no caso dos equipamentos com suporte a vários protocolos de rede, para a MIB-II foi decidido criar uma tabela deste tipo dentro do ramo de cada protocolo de rede, mantendo a tabela `atTable` por questões de compatibilidade.

No ramo `ip` existe a seguinte tabela onde é feito o mapeamento entre o endereço IP e endereço físico, devendo esta ser utilizada em detrimento da tabela `atTable`. A excepção é no caso do equipamento não a suportar.

Tabela 4.3 - Tabela ipNetToMediaTable da MIB-II

ipNetToMediaTable (.1.3.6.1.2.1.4.22)		
ipNetToMediaEntry (1)	ipNetToMediaEntry (1)	Valor identificador do interface onde o mapeamento se encontra activo.
	ipNetToMediaPhysAddress (2)	Endereço físico. Normalmente o endereço MAC.
	ipNetToMediaNetAddress (3)	Endereço IP.
	ipNetToMediaType (4)	Tipo de mapeamento: other (1) invalid (2) - Permite à estação de gestão invalidar o mapeamento dynamic (3) static (4)

Em relação à tabela anterior esta apresenta mais uma coluna, `ipNetToMediaType` que indica o tipo de mapeamento, permitindo invalidar um determinado mapeamento caso seja necessário.

4.2.2 MIB genérica IEEE 802.11

O grupo de trabalho do IEEE responsável pelo desenvolvimento da norma IEEE 802.11 definiu conjuntamente com a norma uma MIB que possibilitaria gerir equipamentos compatíveis com essa mesma norma. A MIB em questão tem o nome IEEE802Dot11 e não se localiza no tradicional ramo de gestão da internet (`iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1)`), mas sim no ramo `iso(1).member-body(2).us(840).ieee802dot11(10036)`.

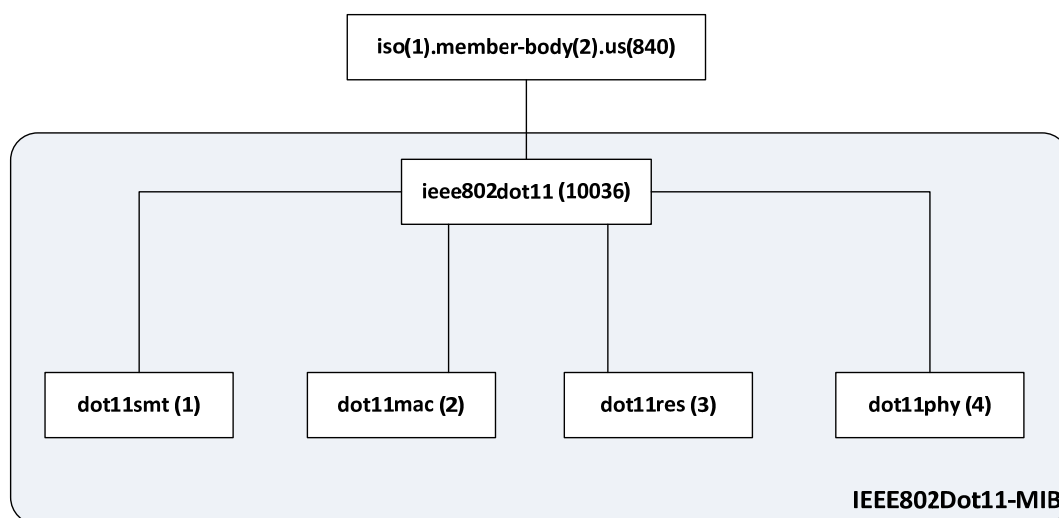


Figura 4.2 - Principais ramos da MIB IEEE802Dot11

Tal como é visível no diagrama anterior, a MIB é composta por quatro ramos principais:

- **dot11smt** - (*Station Management*) Este ramo é constituído por objectos relacionados com a gestão da estação Wi-Fi. Tal como é visível na figura seguinte, o ramo é constituído por seis tabelas, dividindo-o nas categorias de configuração, autenticação e encriptação.

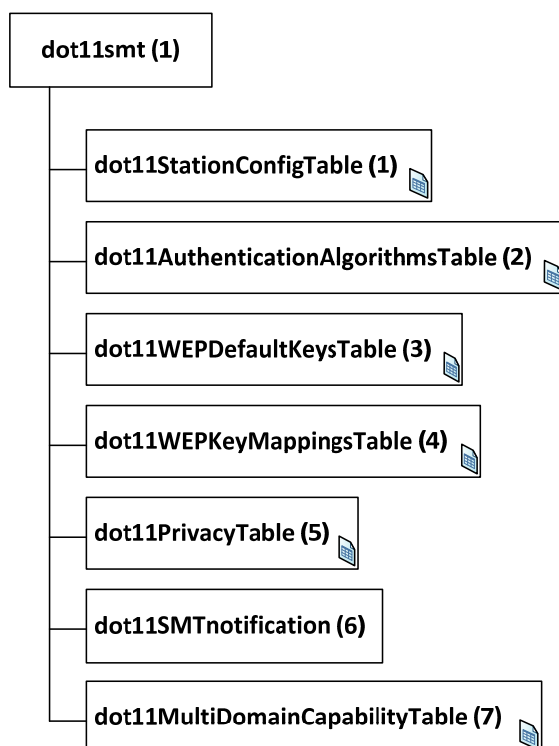


Figura 4.3 - Ramo dot11smt da MIB IEEE802Dot11

Ao analisar as várias tabelas não é difícil identificar as seguintes limitações:

- Na tabela de configuração da estação (dot11StationConfigTable) não foi prevista a situação de um ponto de acesso suportar mais do que um SSID, não sendo possível fazer a gestão usando os objectos lá presentes para uma situação dessas.
- A tabela de autenticação (dot11AuthenticationAlgorithmsTable) apenas prevê dois métodos de autenticação (aberto ou chave partilhada), não suportando o protocolo EAP, necessário para muitas redes empresariais.
- Apenas está previsto o algoritmo de encriptação WEP, não existindo forma de configurar outro algoritmo.

- **dot11mac** - Este é o ramo dedicado à gestão da camada MAC na MIB IEEE802Dot11. Está dividido nas seguintes três tabelas.

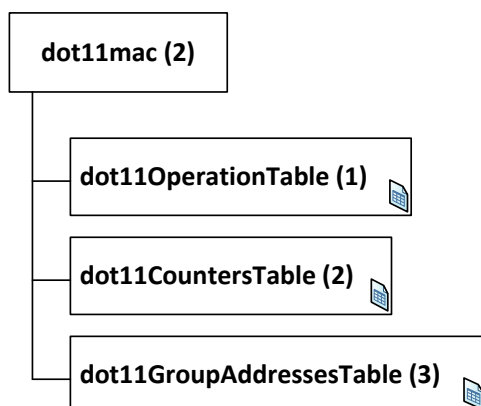


Figura 4.4 - Ramo dot11mac da MIB IEEE802Dot11

A tabela dot11OperationTable possui os parâmetros associados à camada MAC. Permite, por exemplo, alterar alguns parâmetros que controlam as retransmissões de tramas.

A tabela dot11CountersTable possui um conjunto de contadores que permitem fazer algum diagnóstico sobre as falhas ocorridas a nível da camada MAC.

Finalmente a tabela dot11GroupAddressesTable permite ter uma lista de endereços *multicast* para a qual a estação sem fios aceita tramas.

- **dot11res** - (*Resources*) Este ramo é apenas de informação sobre os recursos rádio da estação. É composto por apenas uma tabela onde é possível obter o nome do fabricante, modelo e versão dos interfaces rádio.

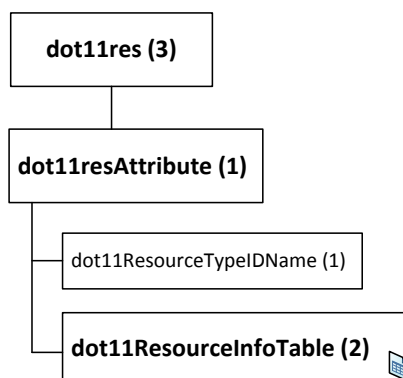


Figura 4.5 - Ramo dot11res da MIB IEEE802Dot11

- **dot11phy** - Este é o ramo onde estão presentes os objectos para a gestão da camada física dos interfaces de rede sem fios presentes na estação.

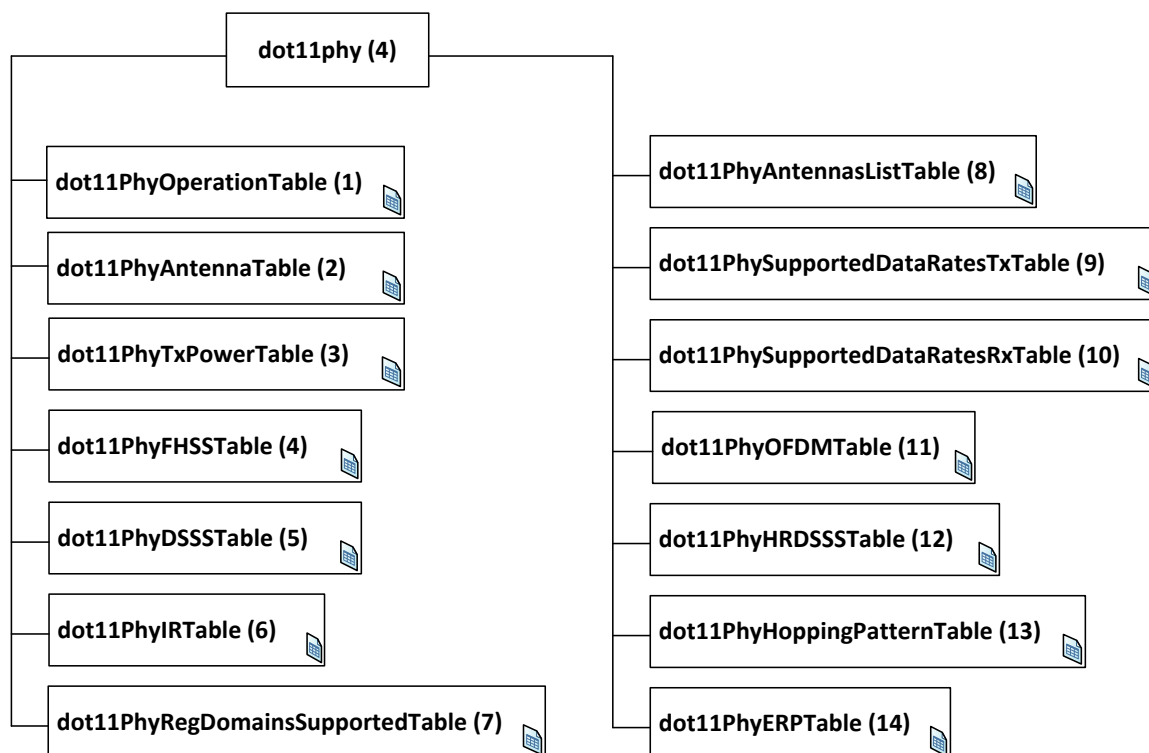


Figura 4.6 - Ramo dot11phy da MIB IEEE802Dot11

Devido às limitações da MIB, principalmente na área de gestão, para muitas situações é necessário complementá-la com objectos de outras MIBs. A solução adoptada pela generalidade dos fabricantes de hardware compatível com a norma IEEE 802.11 foi desenvolver MIBs próprias para resolver as limitações existentes. Nalguns casos baseiam-se nesta e a suas próprias MIBs apenas expandem, incluindo os objectos necessários para a gestão completa do ponto de acesso. Noutros casos ignoram esta MIB e desenvolvem de raiz uma MIB própria.

4.2.3 MIBs Proprietárias

Nesta secção serão apresentadas algumas MIBs proprietárias que serão importantes para a gestão dos equipamentos.

4.2.3.1 Cisco

Os equipamentos deste fabricante são bastante flexíveis permitindo imensas opções de configuração. A gestão através do protocolo SNMP também é muito potente e como tal obriga a que o número de objectos da base de dados de gestão seja enorme. De forma a obter uma boa organização de objectos, o fabricante agrupou-os em inúmeras e diferentes MIBs, possibilitando que diferentes equipamentos partilhem vários grupos de objectos comuns.

Os objectos mais importantes relacionados com a gestão dos equipamentos com suporte da norma IEEE 802.11 estão localizados nas seguintes MIBs:

- CISCO-DOT11-IF-MIB
- CISCO-DOT11-SSID-SECURITY-MIB
- CISCO-DOT11-ASSOCIATION-MIB

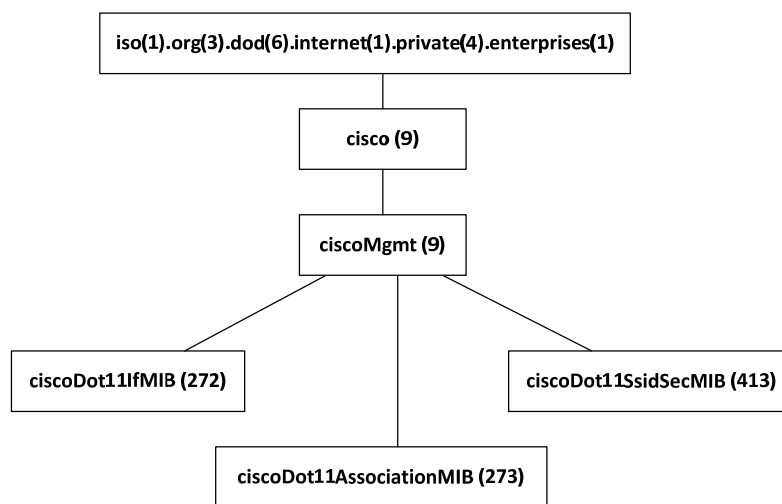


Figura 4.7 - Localização das MIBs proprietárias da Cisco na árvore de gestão

4.2.3.1.1 CISCO-DOT11-IF-MIB

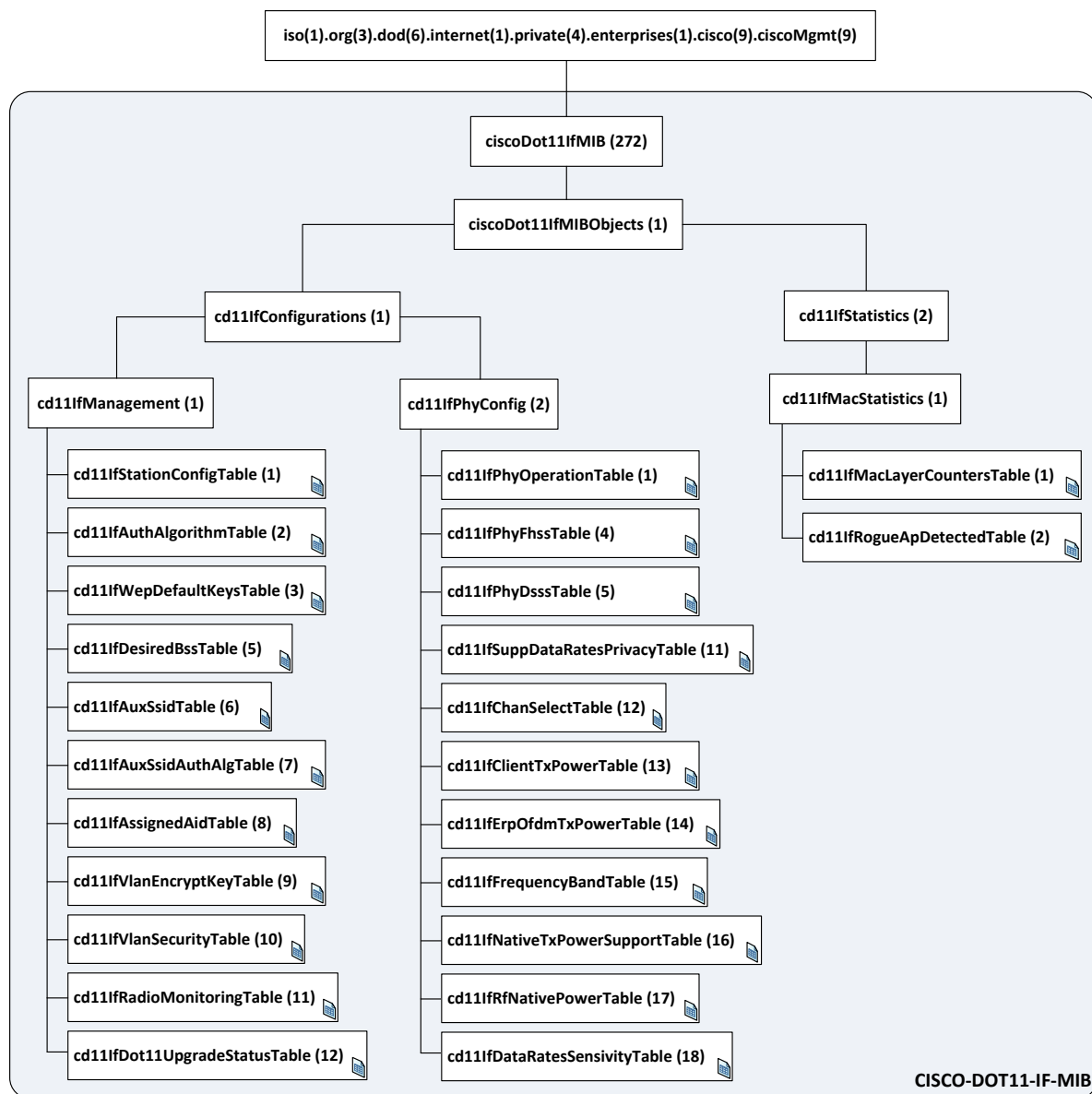


Figura 4.8 - Principais objectos da MIB CISCO-DOT11-IF-MIB

Tal como é possível observar na figura anterior, esta MIB é composta por um grupo de objectos de configuração e outro de informação estatística dos interfaces de rede IEEE 802.11 do ponto de acesso.

Algumas tabelas fazem uma expansão das tabelas existentes na MIB desenvolvida pelo IEEE, contendo apenas os objectos que não se encontram presentes nessa MIB.

4.2.3.1.2 CISCO-DOT11-SSID-SECURITY-MIB

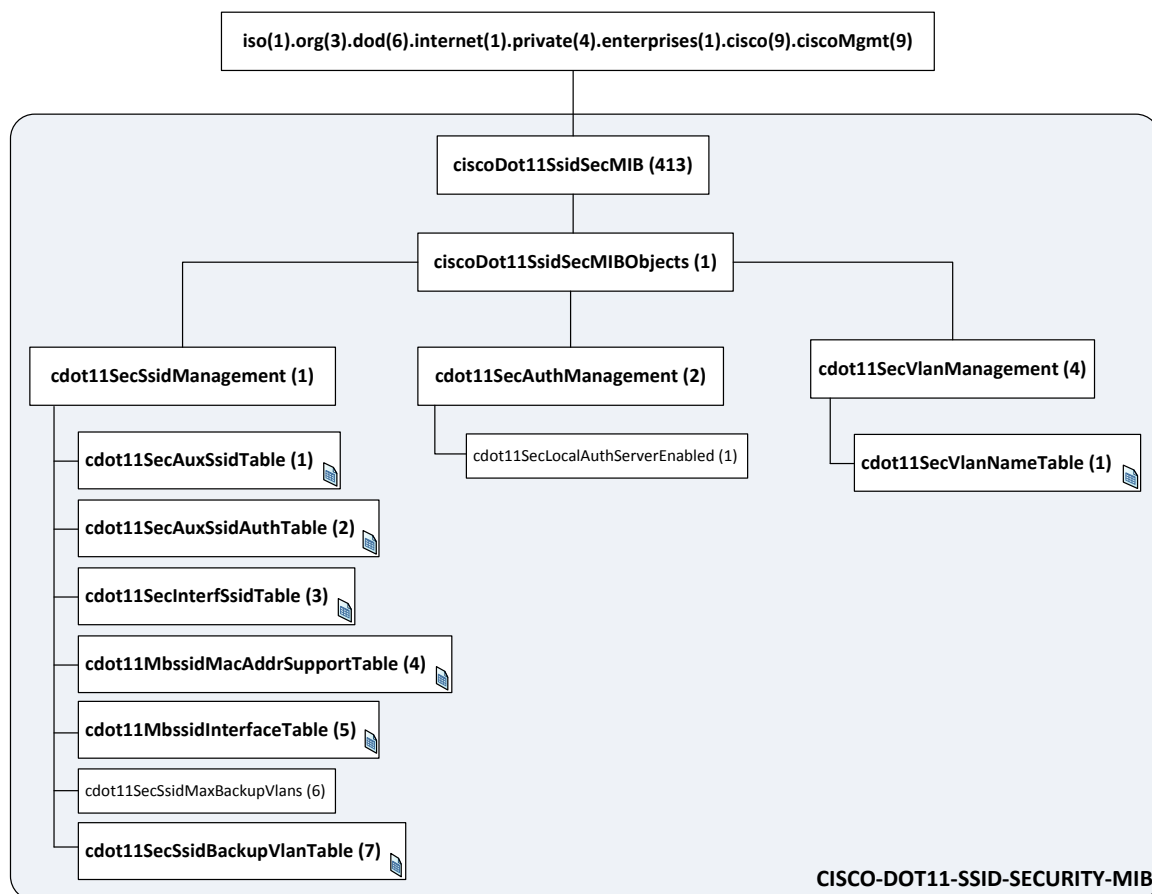


Figura 4.9 - Principais objectos da MIB CISCO-DOT11-SSID-SECURITY-MIB

Esta é uma MIB mais recente que permite complementar a MIB CISCO-DOT11-IF-MIB, especificamente na área de gestão de múltiplos SSIDs e respectivos mecanismos de segurança. Adiciona também a possibilidade de adicionar e remover SSIDs, funcionalidade que não era conseguida através da MIB anterior.

4.2.3.1.3 CISCO-DOT11-ASSOCIATION

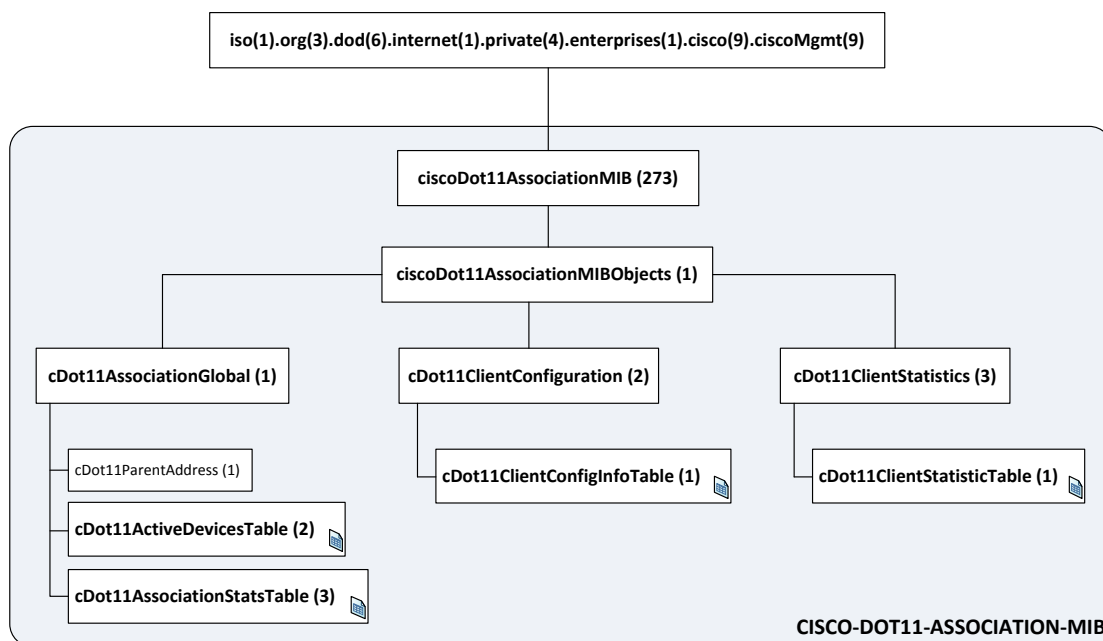


Figura 4.10 - Principais objectos da MIB CISCO-DOT11-ASSOCIATION-MIB

Os objectos da MIB CISCO-DOT11-ASSOCIATION-MIB permitem a obtenção de informação sobre as estações associadas.

Através da tabela `cDot11ActiveDevicesTable`, sob o ramo `cDot11AssociationGlobal` é possível obter o número de estações associadas em cada interface de rede IEEE 802.11 do ponto de acesso.

A tabela `cDot11AssociationStatsTable` fornece informação estatística sobre as associações e dissociações de terminais a cada interface de rede.

Sob os ramos `cDot11ClientConfiguration` e `cDot11ClientStatistics` encontram-se as tabelas `cDot11ClientConfigInfoTable` e `cDot11ClientStatisticTable`, onde é possível obter informação detalhada sobre cada terminal associado ao ponto de acesso. Parâmetros tais como nível de sinal e relação sinal/ruído do sinal recebido da estação terminal, débito máximos permitidos e tempo total da associação do terminal podem ser encontrados nestas duas tabelas.

O índice de cada entrada destas duas tabelas é composto por:

- Valor identificador do interface rádio onde o terminal se encontra associado (`ifIndex`).
- Comprimento e código ASCII, em decimal, de cada um dos caracteres do SSID a que o terminal se encontra associado.

- Valor, em decimal, dos seis octetos do endereço MAC do terminal separados por pontos.

Exemplo:

- ifIndex = 1
- SSID = “teste”
- Endereço MAC do terminal = 12:34:56:78:9A:BC

Origina o seguinte índice na entrada da tabela:

1.5.116.101.115.116.101.18.52.86.120.154.188

Embora um índice tão complexo possa à primeira vista ser complicado de utilizar, torna-se útil quando é pretendido pesquisar uma determinada estação pelo seu endereço MAC, visto que não é necessário retirar todos valores da tabela para fazer a pesquisa. Basta verificar se existe alguma entrada na tabela com esse índice.

4.2.3.1.4 CISCO-CONFIG-COPY-MIB

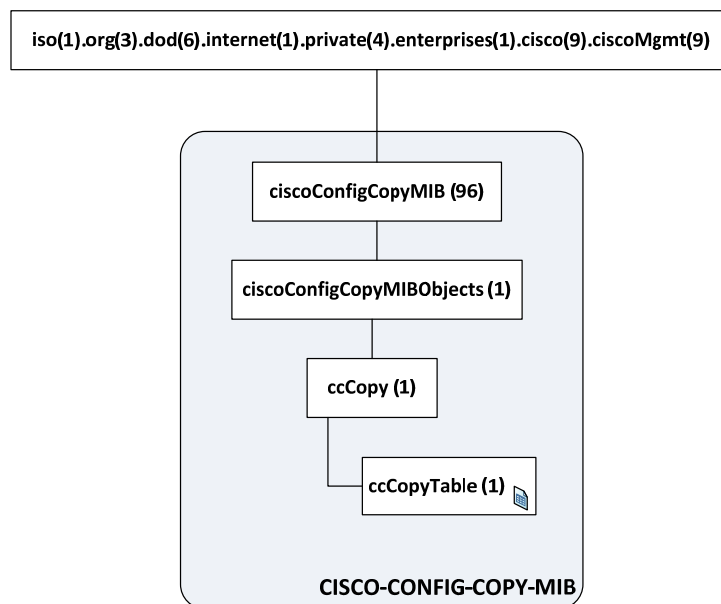


Figura 4.11 - Principais objectos da MIB CISCO-CONFIG-COPY-MIB

As alterações efectuadas à configuração apenas ficam guardadas na configuração corrente do equipamento (*running-config*), sendo necessário copiá-las para a memória não volátil, o que a Cisco chama *startup-config*, de modo a que não sejam perdidas quando for necessário reinicializar o equipamento. Este passo pode ser realizado com recurso à tabela `ccCopyTable` que está presente na MIB proprietária CISCO-CONFIG-COPY-MIB. Para tal, é apenas necessário criar uma entrada na tabela com os parâmetros da cópia. Esta tabela também permite a cópia da configuração actual para um servidor de TFTP ou vice-versa, possibilitando fazer uma cópia de segurança da configuração ou uma reposição de uma configuração previamente guardada.

4.2.3.2 D-Link

Este fabricante optou por não incluir na base de dados de objectos do agente SNMP dos seus pontos de acesso, os objectos da MIB do IEEE, tendo desenvolvido uma MIB própria para todos os aspectos de configuração e monitorização do ponto de acesso sem fios.

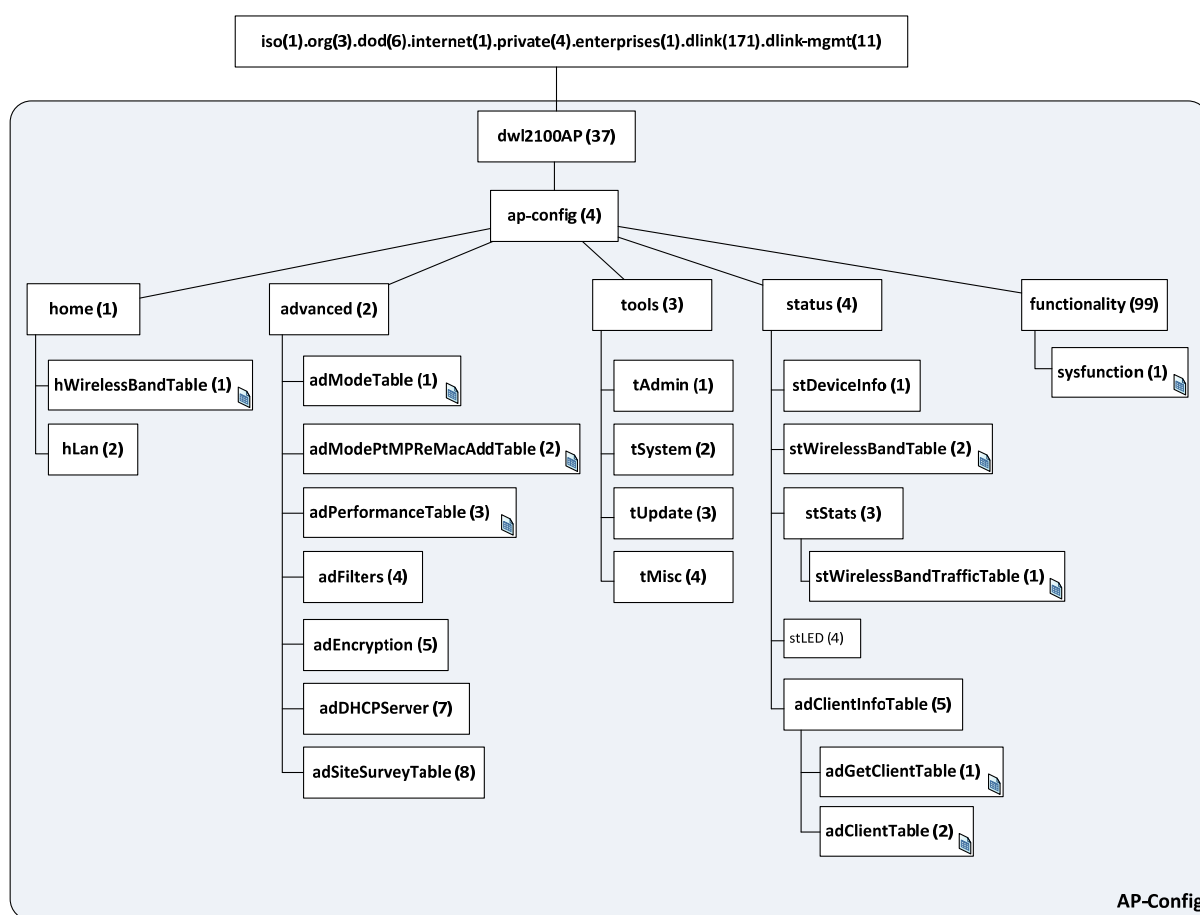


Figura 4.12 - Principais ramos da MIB dos pontos de acesso da D-Link

Apesar do nome do nó dentro do ramo de gestão da D-Link (.1.3.6.1.4.1.171.11) ter o nome de um modelo específico (dwl2100AP), a MIB é igual para vários modelos de pontos de acesso da D-Link.

Capítulo 5

Implementação

Neste capítulo é realizada uma descrição da solução implementada. Compreende também uma secção com uma análise à segurança da solução.

5.1 Localização da solução na Rede Wi-Fi

Apresenta-se de seguida a topologia da rede de um possível cenário para um sistema de gestão da infra-estrutura de rede Wi-Fi.

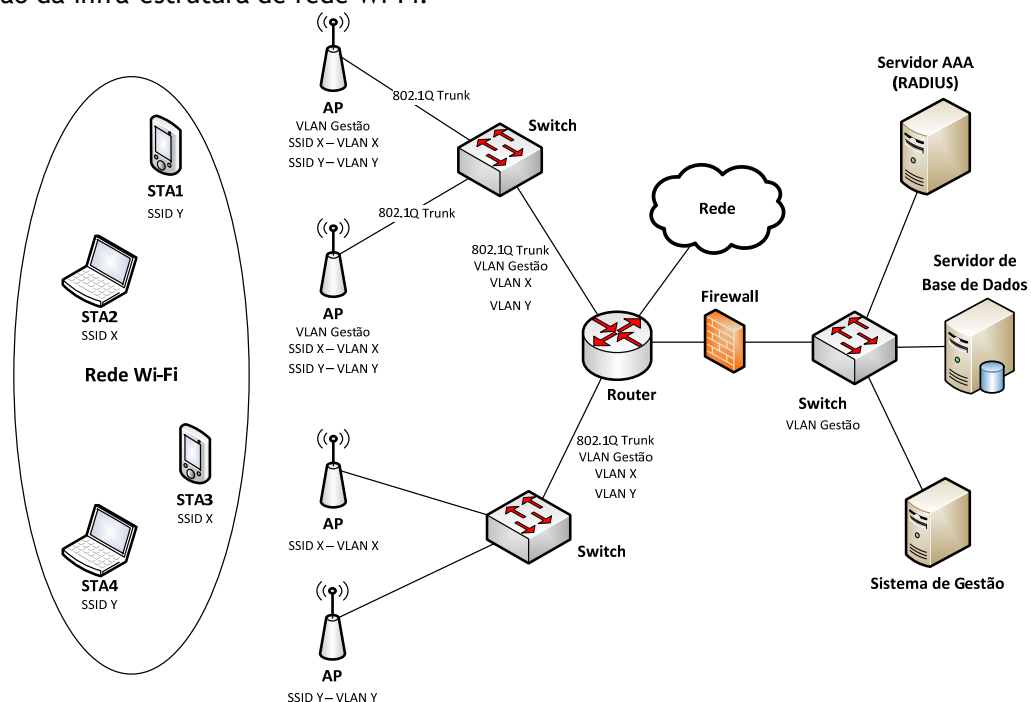


Figura 5.1 - Diagrama com a topologia da rede

Nesta topologia o tráfego dos pontos de acesso é agregado nos vários *switches*, sendo o router responsável pela comutação de pacotes entre as várias sub-redes.

Cada SSID é associado a uma VLAN diferente assim como a sub-redes diferentes, levando a uma separação completa das redes sem fios, tanto a nível 2 como a nível 3. Para o caso dos pontos de acesso que não permitam ter mais do que um SSID nem tenham suporte de VLANs terão de ficar com o seu endereço de gestão na sub-rede associada ao seu SSID.

Por questões de segurança dos servidores de gestão, existe uma firewall à entrada desta rede de modo a bloquear o acesso dos utilizadores das redes Wi-Fi a esta sub-rede, permitindo apenas a comunicação entre os pontos de acesso e o servidor RADIUS e a comunicação do sistema de gestão com os pontos de acesso.

Para o acesso dos utilizadores à rede assim como para a gestão e monitorização da rede, estão presentes na rede de gestão os seguintes servidores:

Servidor AAA - Este servidor é responsável pela autenticação dos terminais e a respectiva autorização do seu acesso à rede. Também é responsável pela contabilização de volume de tráfego e tempo de cada sessão. O protocolo mais utilizado e suportado pela maioria dos equipamentos é o protocolo RADIUS (*Remote Authentication Dial In User Service*).

Servidor de Base de Dados - A existência de uma base de dados centralizada permite que os seus dados sejam utilizados por vários servidores e/ou serviços. Neste caso específico, é utilizada pelo servidor RADIUS e pela estação de gestão.

Sistema de Gestão - Neste sistema é realizada a monitorização e gestão da rede. Está igualmente incluído o interface com o utilizador onde são apresentados os dados da monitorização efectuada, permitindo ao utilizador efectuar alterações na configuração dos equipamentos da rede.

5.2 Tecnologias escolhidas para a implementação da solução

O protótipo foi implementado com recurso a várias ferramentas de software de domínio público. A linguagem de programação escolhida foi PHP (*Hypertext Preprocessor*), pela sua extensa biblioteca de funções assim como pela capacidade de programação orientada a objectos. Tanto o interface com o utilizador como as aplicações que correm periodicamente sem intervenção do utilizador utilizarão a mesma linguagem de programação permitindo a existência de bibliotecas comuns.

O interface com o utilizador assenta sobre uma base Web, levando a que apenas seja necessário um *browser* para o utilizar.

Servidor de Base de Dados

Para servidor de Base de Dados é utilizado o software MySQL, pois devido à sua robustez e performance é dos servidores de base de dados mais utilizados.

Biblioteca e ferramentas SNMP

As funções de SNMP existentes no PHP utilizam as bibliotecas do software Net-SNMP. Este pacote inclui um agente de SNMP (que não é utilizado nesta solução), uma aplicação que permite receber as notificações de SNMP de outros agentes (*snmptrapd*) e várias ferramentas que permitem retirar e alterar informação dos equipamentos com suporte de SNMP.

Servidor RADIUS

Foi escolhido o pacote de software FreeRADIUS pois é bastante modular permitindo trabalhar com vários sistemas de gestão de bases de dados, incluindo o servidor MySQL.

Para registo do histórico dos valores que serão recolhidos é utilizada a ferramenta RRDTool, pois é bastante eficiente em tarefas deste tipo. Para além disto possui a capacidade de gerar gráficos que facilitam a visualização da evolução dos valores ao longo do tempo.

5.3 Arquitectura do sistema de gestão

O sistema de gestão é responsável por fazer o interface entre os equipamentos e o utilizador. Para tal terá que comunicar com os equipamentos através do protocolo de gestão SNMP e, para determinadas operações que não possam ser realizadas com recurso a este protocolo pode recorrer ao terminal dos mesmos através do protocolo Telnet ou SSH (*Secure Shell*). Pode também receber notificações assíncronas dos equipamentos através de Traps SNMP, devendo classificá-las, gerar um evento e guardar esse registo numa base de dados de eventos.

Para a autenticação dos utilizadores, autorização do seu acesso à rede e contabilização da utilização dos recursos, o sistema de gestão será apoiado por um servidor AAA (*Authentication, Authorization and Accounting*) que será responsável por essas tarefas, sendo a comunicação entre os pontos de acesso e o servidor AAA é efectuada através do protocolo RADIUS. O interface entre o sistema de gestão e o servidor AAA é realizado utilizando bases de dados partilhadas por estes dois sistemas, nomeadamente a base de dados de autenticação e contabilização.

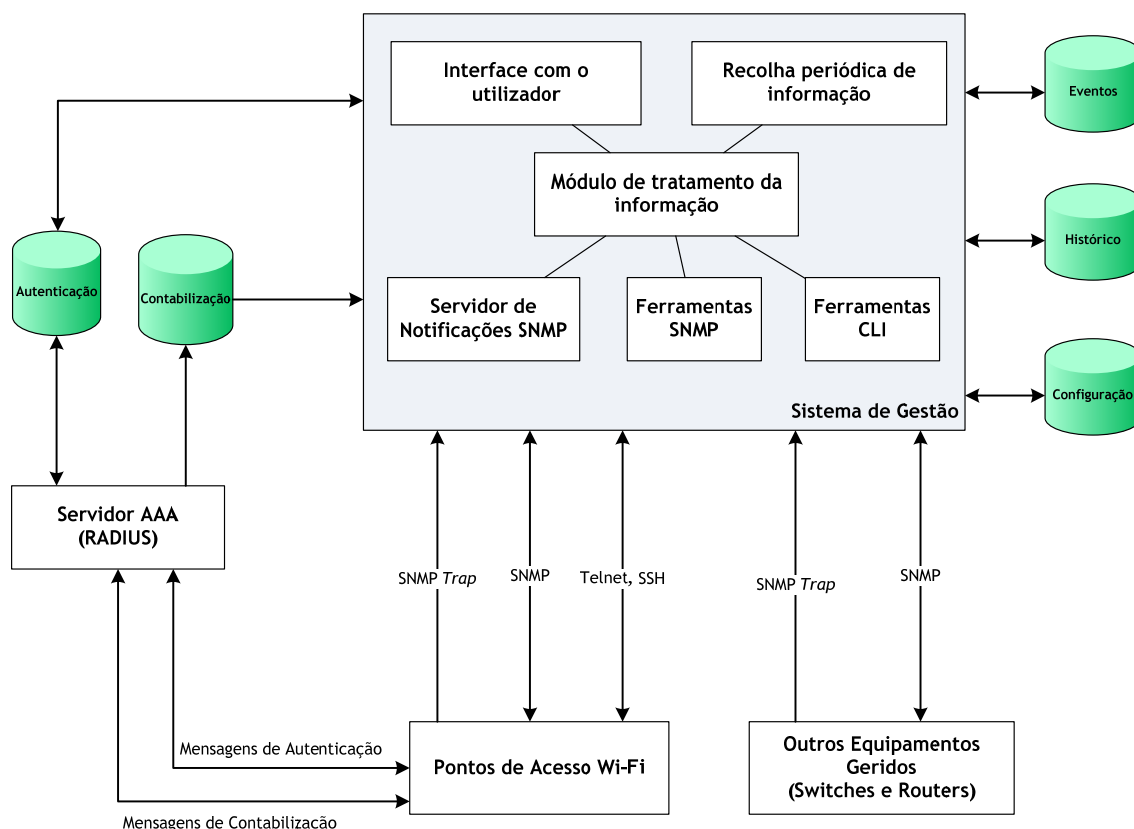


Figura 5.2 - Arquitectura geral do sistema de gestão

De forma a tornar o sistema mais flexível em termos de configuração, a maioria das configurações fica armazenada numa base de dados de configuração, permitindo a existência de um interface simples de manipulação da configuração.

Segue-se uma ilustração que pormenoriza o módulo de tratamento da informação do sistema de gestão, possibilitando visualizar a interacção entre os vários módulos e bases de dados do sistema de gestão.

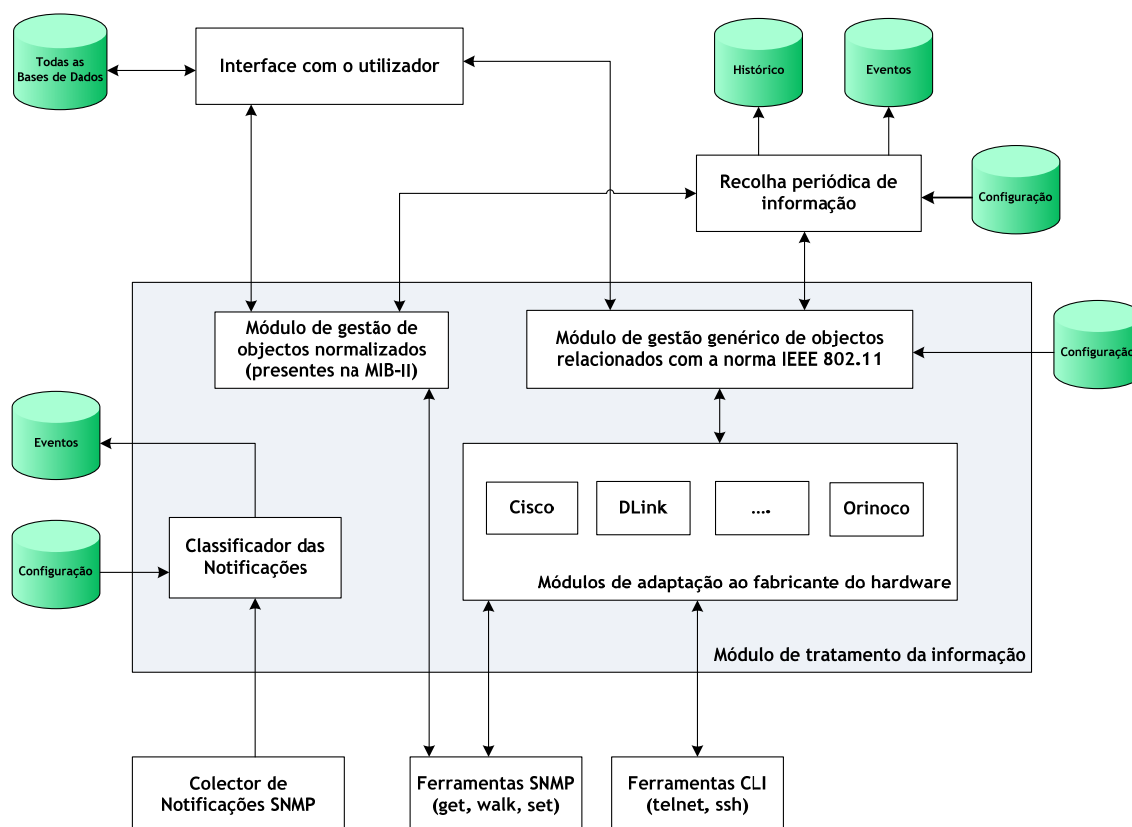


Figura 5.3 - Detalhe do módulo de tratamento da informação

O módulo de tratamento da informação actua como uma camada intermédia responsável por normalizar a informação recolhida dos equipamentos através das ferramentas SNMP ou até mesmo através da consola do equipamento, utilizando a CLI (*Command Line Interface*) do mesmo.

Devido à pouca uniformização dos objectos relacionados com a norma IEEE 802.11, a solução desenvolvida utiliza um conjunto de módulos que fazem a adaptação ao fabricante do hardware, utilizando os objectos próprios de cada fabricante, tornando o processo transparente para as camadas superiores. Sempre que for necessário suportar um novo *hardware* basta adicionar um módulo de adaptação, não sendo preciso alterar nada nas

camadas superiores. Para tal é apenas necessário indicar na base de dados de configuração a existência desse novo módulo e quais os modelos e/ou fabricantes que o mesmo suporta.

Paralelamente existe o classificador de notificações que é chamado sempre que o colector de notificações SNMP receber alguma notificação SNMP de algum equipamento, tratando de gerar um evento com base na configuração que existe na base de dados de configuração e inserindo-o na base de dados de eventos.

Foram também implementados alguns módulos que correm de forma periódica recolhendo informação dos vários equipamentos para fazer um histórico de determinados valores, podendo gerar eventos de alerta em situações onde os valores recolhidos estejam fora de alguns limites previamente definidos pelo utilizador.

5.3.1 Módulo de gestão de objectos presentes na MIB-II

Este módulo faz parte da biblioteca de funções que permitem recolher e alterar parâmetros nos equipamentos através do protocolo SNMP, sendo o seu objectivo implementar os métodos para a gestão de objectos presentes na MIB-II. Ao contrário do módulo seguinte, módulo de gestão de objectos relacionados com a norma IEEE 802.11, este não precisa de uma camada de abstracção do fabricante do *hardware*, pois todos os equipamentos suportam a MIB-II, sendo possível efectuar as operações de uma forma uniforme, independentemente do *hardware*.

Embora a MIB-II possua uma enorme quantidade de objectos, muitos dos problemas enunciados anteriormente são resolvidos à custa de poucos objectos. Na tabela seguinte são apresentados os métodos implementados neste módulo que trabalham com objectos desta MIB.

Tabela 5.1 - Métodos implementados no módulo MIB-II

Nome do método	Descrição
<code>getSysContact</code>	Este método, tal como o próprio nome sugere, retorna o valor do objecto <code>sysContact.0</code> presente no ramo <code>system</code> da MIB-II. Normalmente o valor deste objecto representa o contacto da pessoa responsável pelo equipamento.
<code>setSysContact</code>	Este método permite efectuar a alteração do valor do objecto retornado pelo método anteriormente descrito. Terá que receber como argumento uma <i>string</i> com o novo valor. O seu valor de retorno deverá ser booleano, indicando o sucesso ou falha da operação.
<code>getSysDescr</code>	Este método retorna o valor do objecto <code>sysDescr.0</code> do ramo <code>system</code> . Este valor contém uma breve descrição do equipamento. Tipicamente contém o nome do fabricante, modelo, versão de <i>software</i> e revisão do <i>hardware</i> numa <i>string</i> .
<code>getSysName</code>	Este método retorna o valor do objecto <code>sysName.0</code> do ramo <code>system</code> . O valor é normalmente o <i>hostname</i> do equipamento.
<code>setSysName</code>	Este método permite efectuar a alteração do valor do objecto retornado pelo método anteriormente descrito. Terá que receber como argumento uma <i>string</i> com o

	novo valor. O seu valor de retorno deverá ser booleano, indicando o sucesso ou falha da operação.
getSysObjectID	Este método retorna o valor do objecto <code>sysObjectID.0</code> do ramo <code>system</code>.
getSysUptime	Este método retorna o valor do objecto <code>sysUptime.0</code> do ramo <code>system</code>. Esse valor dá a indicação do tempo, em centésimas de segundo, desde que o agente SNMP do equipamento foi reinicializado.
getAtTable	Este método permite fazer uma recolha da tabela de ARP do equipamento, através da tabela <code>atTable</code> presente no ramo <code>at</code> da MIB-II. O seu valor de retorno é um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o endereço IP e o seu valor é outra <i>string</i> com o endereço MAC associado a esse endereço IP. Segue-se um exemplo: <pre> Array ([172.16.2.30] => 001e14b68c40 [172.16.2.40] => 001e147c8fc0) </pre>
getIfTable	Este método permite fazer uma recolha da tabela de interfaces de rede do equipamento, através da tabela <code>ifTable</code>. O seu valor de retorno é um <i>array</i> associativo onde a chave de cada elemento é o índice do interface e o seu valor é outro <i>array</i> com os valores das várias colunas (da tabela <code>ifTable</code>) associadas a esse interface. Segue-se um exemplo: <pre> Array ([1] => Array ([2] => FastEthernet 0/1 [3] => 6 [4] => 1500 [5] => 100000000 [6] => 001e14b68c01 </pre>

	<pre> [7] => 1 [8] => 1 ...)) </pre>
<code>getIfInOctets</code>	O objectivo deste método é permitir fazer a leitura de uma das linhas da coluna <code>ifInOctets</code> da tabela <code>ifTable</code> , utilizando como argumento o nome do interface.
<code>getIfOutOctets</code>	Este método permite fazer a leitura de uma das linhas da coluna <code>ifOutOctets</code> da tabela <code>ifTable</code> . O argumento deverá ser o nome do interface.
<code>getIfInErrors</code>	O objectivo deste método é permitir fazer a leitura de uma das linhas da coluna <code>ifInErrors</code> da tabela <code>ifTable</code> , utilizando como argumento o nome do interface.
<code>getIfOutErrors</code>	Este método permite fazer a leitura de uma das linhas da coluna <code>ifOutErrors</code> da tabela <code>ifTable</code> . O argumento deverá ser o nome do interface.

Os últimos quatro métodos descritos permitem recolher determinados valores de um interface específico. O seu objectivo é possibilitar ao módulo de recolha periódica de informação a recolha de alguns valores, que permitem o cálculo da ocupação do interface, assim como a sua taxa de erros.

Sempre que seja necessário referenciar um interface de rede foi escolhido referenciá-lo através do seu nome (campo `ifDescr` na tabela `ifTable`), e não através do seu índice (campo `ifIndex`), pois só assim se consegue garantir que a leitura dos valores está a ser realizada no interface correcto. Isto é devido à possibilidade do próprio agente SNMP do equipamento poder alterar os índices dos interfaces aquando de uma alteração da *firmware* ou alteração no *hardware*.

Qualquer um dos métodos poderá retornar o valor booleano falso em caso de erro na realização da operação. Nesse caso é também preenchida uma *string* com a descrição textual do erro, para que a aplicação que tenha invocado o método torne a mensagem de erro visível para o utilizador.

5.3.2 Módulo de gestão de objectos relacionados com a norma IEEE 802.11

Este módulo é responsável pela escolha do módulo de adaptação ao fabricante e pela chamada dos métodos presentes nesses módulos. Essa escolha é feita com base no valor do objecto `sysObjectID`. Este valor é um OID que permite saber qual é o equipamento que está a ser gerido, tendo cada modelo de equipamento um valor identificador dentro da MIB do fabricante.

De forma a que seja mais fácil de adicionar ou remover módulos de adaptação ao fabricante, tornando o sistema mais flexível, a associação entre os valores do objecto `sysObjectID` e o nome do módulo correspondente fica numa tabela na base de dados de configuração.

Foram definidos os seguintes métodos que deverão ser implementados pelos módulos de adaptação ao fabricante do hardware, retornando a informação no formato indicado na tabela seguinte.

Tabela 5.2 - Métodos que deverão ser implementados pelos módulos de adaptação ao fabricante

Nome do método	Descrição
<code>getNumOfAssociatedClients</code>	Este método deverá retornar o número total de estações associadas ao ponto de acesso.
<code>getAssociatedClients</code>	Este método é utilizado para determinar quais as estações que estão associadas aos SSIDs de um determinado ponto de acesso assim como alguns detalhes dessas mesmas estações. Os detalhes mais importantes que são fornecidos pela generalidade dos pontos de acesso são: • SSI (<i>Signal Strength Indicator</i>) - Indicador do nível de sinal recebido da última trama enviada pela estação em questão. A unidade deste parâmetro é normalmente dependente da implementação do fabricante, devendo ser retornada juntamente com o valor. • Relação sinal/ruído - Indicador da relação sinal ruído da última trama enviada pela estação em questão. • Débito máximo negociado com a estação. O método deverá retornar um <i>array</i> associativo no formato indicado a seguir. Os detalhes que não sejam

	disponibilizados pelo ponto de acesso podem ser omitidos na resposta. <pre> Array ([Nome do Interface] => Array ([Nome do SSID] => Array ([Endereço MAC] => Array ([SSI] => Valor [DataRate] => Valor [SNR] => Valor))))))) </pre>
Canais de operação dos interfaces rádio	
<code>getCurrentChannel</code>	Este método é utilizado para saber qual o canal actual associado a cada um dos interfaces do ponto de acesso. Deverá retornar um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o nome do interface e o seu valor é o canal associado a esse interface.
<code>setChannel</code>	O objectivo deste método é possibilitar a alteração do canal de um determinado interface do ponto de acesso. Terá que receber como primeiro argumento uma <i>string</i> com o nome do interface, sendo o segundo valor o canal desejado. O seu valor de retorno deverá ser booleano, indicando o sucesso ou falha da operação.
<code>setAutoChannel</code>	Este método permite definir o canal de operação de um determinado interface rádio do ponto de acesso. Terá que receber como primeiro argumento uma <i>string</i> com o nome do interface, sendo o segundo valor

	o canal desejado. O valor do canal deverá ser um dos valores retornados pelo método <code>getChannelList</code>. O seu valor de retorno deverá ser booleano, indicando o sucesso ou falha da operação.
<code>getChannelList</code>	Este método permite obter uma lista dos canais suportados por cada interface rádio. Deverá retornar um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o nome do interface e o seu valor é outro <i>array</i> com os canais suportados por esse interface. Se o interface tiver a opção de escolha automática do canal de operação também deverá ser incluída na lista. Exemplo do <i>array</i> que deverá ser retornado pelo método: <pre> Array ([Nome do Interface] => Array ([1] => 1 [2] => 2 [3] => 3 ... [Auto] => Auto)) </pre>
<code>isCurrentChannelAuto</code>	Este método permite determinar se o canal actual de cada interface rádio foi atribuído de uma forma automática ou manual. Deverá retornar um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o nome do interface e o seu valor é booleano, tomando o valor verdadeiro caso esse interface tenha a escolha do canal em modo automático.
Potência dos interfaces rádio	

<code>getCurrentPowerLevel</code>	Este método é utilizado para saber qual a potência de emissão actual associada a cada um dos interfaces do ponto de acesso. Deverá retornar um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o nome do interface e o seu valor é a potência de emissão associada a esse interface. O valor deverá conter a unidade utilizada, visto que também depende da implementação do fabricante.
<code>getPowerLevels</code>	Este método permite obter uma lista com os valores de potência de emissão de cada interface rádio. Deverá retornar um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o nome do interface e o seu valor é outro <i>array</i> com os valores de potência suportados por esse interface. As chaves deste segundo <i>array</i> deverão ser os valores que o método <code>setPowerLevel</code> deverá receber. Exemplo do <i>array</i> que deverá ser retornado pelo método: <pre>Array ([Nome do Interface] => Array ([1] => 1 mW [2] => 2 mW [3] => 10 mW ...))</pre>
<code>setPowerLevel</code>	O objectivo deste método é possibilitar a alteração da potência de emissão de um determinado interface do ponto de acesso. Terá que receber como primeiro argumento uma <i>string</i> com o nome do interface, sendo o segundo valor um dos valores da lista retornada pelo método <code>getPowerLevels</code>. O seu valor de retorno deverá ser booleano, indicando o sucesso ou falha da operação.

Débitos máximos dos interfaces rádio	
getCurrentMaxDataRate	Este método é utilizado para saber qual o débito máximo configurado em cada um dos interfaces rádio do ponto de acesso. Deverá retornar um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o nome do interface e o seu valor é o débito máximo associado a esse interface.
getMaxDataRates	Este método permite obter uma lista com os valores de débito máximo de cada interface rádio. Deverá retornar um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o nome do interface e o seu valor é outro <i>array</i> com os valores de potência suportados por esse interface. As chaves deste segundo <i>array</i> deverão ser os valores que o método <code>setMaxDataRates</code> deverá receber. <pre> Array ([Nome do Interface] => Array ([1] => 1 Mb/s [2] => 2 Mb/s [3] => 11 Mb/s ...)) </pre>
setMaxDataRates	O objectivo deste método é possibilitar a alteração do débito máximo de um determinado interface do ponto de acesso. Terá que receber como primeiro argumento uma <i>string</i> com o nome do interface, sendo o segundo valor um dos valores da lista retornada pelo método <code>getMaxDataRates</code>. O seu valor de retorno deverá ser booleano, indicando o sucesso ou falha da operação.

SSIDs	
getSSIDs	Este método permite obter a associação dos SSIDs aos interfaces do ponto de acesso. Deverá retornar um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o nome do interface e o seu valor é outro array com os SSIDs associados a esse interface. Exemplo do <i>array</i> que deverá ser retornado pelo método: <pre> Array ([Nome do Interface] => Array ([0] => SSID1 [1] => SSID2)) </pre>
getSSIDDetails	Este método é utilizado para determinar os parâmetros de configuração e segurança de cada SSID do ponto de acesso. Deverá retornar um <i>array</i> associativo onde a chave de cada elemento é uma <i>string</i> com o nome do SSID e o seu valor é outro <i>array</i> com os parâmetros desse SSID. Os parâmetros que deverão ser retornados são: • Authentication - Método de autenticação utilizado no SSID (Open, Shared Key ou EAP). • Encryption - Mecanismo de cifra de tramas utilizado (None, WEP, TKIP ou AES). • Broadcast - Valor booleano indicando se o ponto de acesso está a efectuar a difusão do nome do SSID. • VLAN - Identificador da VLAN associada a esse SSID. Podem ser omitidos alguns parâmetros, caso não seja possível a sua obtenção. Exemplo do <i>array</i> que deverá ser retornado pelo

	método: <pre>Array ([SSID1] => Array ([Authentication] => Shared Key [Encryption] => WEP [Broadcast] => true [VLAN] => 1))</pre>
<code>renameSSID</code>	Este método permite fazer a alteração do nome de um SSID no ponto de acesso. Terá que receber como primeiro argumento o nome do SSID a ser alterado e como segundo argumento o novo nome do SSID. O seu valor de retorno deverá ser booleano, indicando o sucesso ou falha da operação.

Tal como acontece no módulo descrito anteriormente, qualquer um dos métodos poderá retornar o valor booleano falso, devendo nessa situação ser preenchida uma *string* com a descrição textual do erro.

5.3.3 Classificador de notificações

Os equipamentos podem enviar notificações para o sistema de gestão de uma forma assíncrona para que sejam feitos registos de situações especiais. As notificações são enviadas através do protocolo SNMP sob a forma de *traps* SNMP, sendo recebidas pelo colector de notificações existente no sistema de gestão. Devido à quantidade e diversidade de notificações que podem ser recebidas por um sistema de gestão inserido numa rede com alguma dimensão, é desejável que as mesmas sejam classificadas de acordo com a sua categoria e importância.

O objectivo deste módulo é efectuar essa classificação, gerando um evento de acordo com uma configuração existente na base de dados de configuração. A esse evento está associada uma categoria e uma importância, podendo conter uma mensagem que descreva a notificação utilizando a informação que lá possa estar contida na notificação recebida. Também, de uma forma adicional, e se assim estiver configurado na base de dados, este módulo pode executar outro programa que efectue uma determinada acção (por exemplo enviar um email ou SMS para a pessoa responsável pelo equipamento).

Segue-se um fluxograma que demonstra os traços gerais do funcionamento deste módulo.

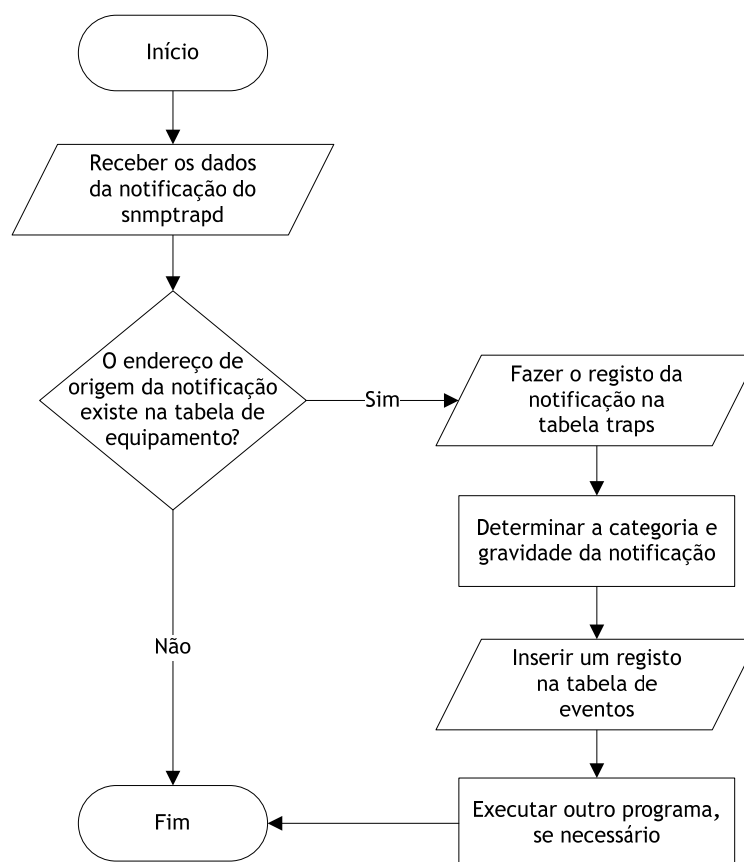


Figura 5.4 - Fluxograma do funcionamento do Classificador de notificações

Qualquer *trap* SNMP recebido pelo colector de notificações (*daemon snmptrapd* do pacote Net-SNMP) é enviado para este módulo. Tal como é evidenciado no fluxograma anterior, a primeira acção que o módulo faz é tentar identificar o equipamento que enviou a notificação. Se o endereço de origem da notificação não estiver na tabela de equipamento, a notificação é descartada, oferecendo uma maior segurança à solução.

A classificação da notificação é feita com base no valor do objecto `snmpTrapOID`, que deverá existir sempre numa notificação SNMPv2. Para o caso de notificações utilizando o PDU definido na primeira versão do protocolo SNMP o colector de notificações utilizado converte automaticamente para o formato utilizado no protocolo SNMPv2, sendo o processo completamente transparente para este módulo.

Na base de dados do protótipo desenvolvido foi utilizado o seguinte modelo relacional para as tabelas utilizadas por este módulo.

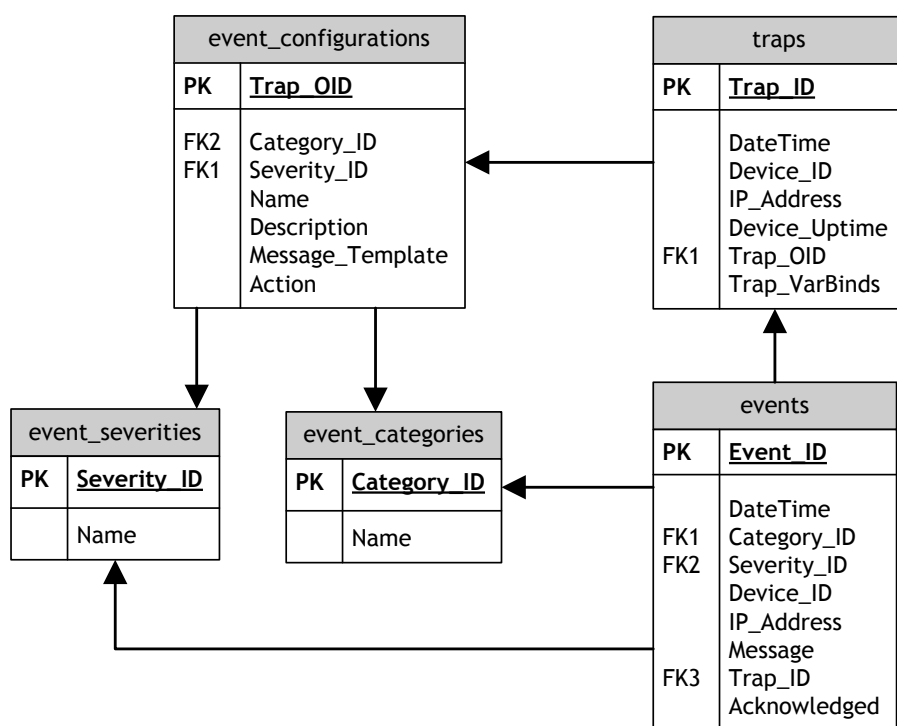


Figura 5.5 - Modelo relacional das tabelas utilizadas pelo módulo Classificador de notificações

5.3.4 Recolha Periódica de Informação

Os módulos de recolha periódica de informação têm como principal objectivo recolher e efectuar registos de valores e parâmetros associados aos equipamentos geridos, gerando um histórico a partir desses valores. A partir desse histórico torna-se possível detectar situações de falha, permitindo ao sistema gerar eventos de alerta.

Na solução apresentada foram desenvolvidos os seguintes três módulos:

- Monitorização dos equipamentos
- Recolha da tabela de ARP dos *routers*
- Recolha da lista de estações associadas

5.3.4.1 Monitorização dos equipamentos

Este módulo foi desenvolvido para efectuar a recolha de valores dos equipamentos, verificar se estão dentro de certos limites e guardar o registo para que possam ser visualizados no interface com o utilizador sob uma forma gráfica.

Durante o seu desenvolvimento foi tomada em consideração a flexibilidade que um módulo destes precisa de ter, pois deverá ser fácil de adicionar novos parâmetros para monitorização.

A implementação desenvolvida recorre a um *script* que corre periodicamente.

A primeira tarefa que este módulo efectua é verificar qual o estado de cada equipamento, fazendo um registo de um evento no caso de alguma alteração de estado de algum equipamento. Esta tarefa permite, por exemplo, detectar a perda de conectividade de um equipamento com a rede, ficando registado num histórico de eventos a falha.

Após essa primeira fase, segue-se a recolha de valores dos equipamentos. Essa recolha é feita de acordo com uma configuração existente numa tabela de configuração presente no SGBD. Os seguintes parâmetros existentes na tabela de configuração indicam a forma como o módulo terá que executar a recolha de um determinado valor:

- **Module** - Módulo a utilizar. Na implementação desenvolvida pode ser utilizado o módulo `MIB-II` ou `IEEE802dot11`.
- **Method** - Método que deverá ser executado.
- **Arguments** - Argumentos que sejam necessários passar ao método.

Para o arquivo dos valores recolhidos este módulo recorre ao pacote de software `RRDTool`. Esta ferramenta usa o conceito de base de dados circular (daí o seu nome de *Round Robin Database Tool*), armazenando um número fixo de registos.

Podem existir várias bases de dados, sendo cada uma armazenada num ficheiro que toma a designação de *Round Robin Archive* (RRA). Dentro desse ficheiro podem existir vários registos de valores, *Data Sources* (DS), tendo cada um, as seguintes propriedades:

- **Nome** (*DSName*) - Nome identificador do registo.
- **Tipo** (*DSType*) - Tipo de valores que são lidos para o registo. Na implementação desenvolvida foram considerados os seguintes tipos:
 - **GAUGE** - Para a leitura de valores que podem aumentar ou diminuir entre leituras consecutivas. Por exemplo: número de estações associadas a um ponto de acesso, canal de um ponto de acesso.
 - **COUNTER** - Para a leitura de valores que são sempre crescentes entre leituras consecutivas, excepto quando o valor máximo é atingido ou quando o agente SNMP é reiniciado. O valor armazenado é a taxa de variação entre leituras consecutivas. Por exemplo: a taxa de variação do número de octetos enviados ou recebidos por um interface de rede.
- **Valor mínimo** (Min) - Este é o valor mínimo que o registo aceita. As leituras que retornem valores menores do que este são ignoradas.
- **Valor máximo** (Max) - Este é o valor máximo que o registo aceita. As leituras que retornem valores maiores do que este são ignoradas.

Após a recolha dos valores, e de uma forma opcional, podem ser feitas algumas verificações a esses valores. Se algum dos valores não se encontrar dentro de um intervalo definido na configuração durante um número de leituras consecutivas (número este também definido na configuração), o módulo responsabiliza-se de gerar um evento no histórico do equipamento de forma a relatar essa situação. Isto torna-se útil para, por exemplo, gerar um evento de alerta quando um ponto de acesso estiver com um número elevado de estações associadas, ou o seu interface de rede estiver com uma ocupação elevada.

datasources	
PK	<u>Datasource_ID</u>
	Device_ID RRA DSName DSType Min Max Module Method Arguments Threshold_Min Threshold_Max Threshold_Count Threshold_CurrentCount

Figura 5.6 - Tabela utilizada pelo módulo de monitorização dos equipamentos

5.3.4.2 Recolha da tabela de ARP dos routers

O objectivo deste módulo é fazer o registo da associação entre endereço IP e endereço MAC das estações associadas aos pontos de acesso, de forma a que seja possível identificar uma estação pelo endereço IP utilizado num determinado momento.

A implementação desenvolvida recorre a um *script* que corre periodicamente. Utiliza o método `getAtTable`, existente no módulo de gestão de objectos presentes na MIB-II, para recolher a tabela de ARP de cada router. Para que seja mantido um registo temporal com as associações entre endereço IP e endereço MAC é utilizada a seguinte tabela no SGBD:

iptomac	
PK	<u>IP Address</u>
PK	<u>MAC Address</u>
PK	<u>FirstSeen</u>
	LastSeen

Figura 5.7 - Tabela utilizada pelo módulo de recolha da tabela de ARP dos routers

As colunas `FirstSeen` e `LastSeen` representam o período de tempo em que a associação se manteve válida.

Durante o processo de recolha da tabela de ARP do equipamento cada entrada da tabela de ARP é sujeita ao tratamento apresentado no fluxograma seguinte.

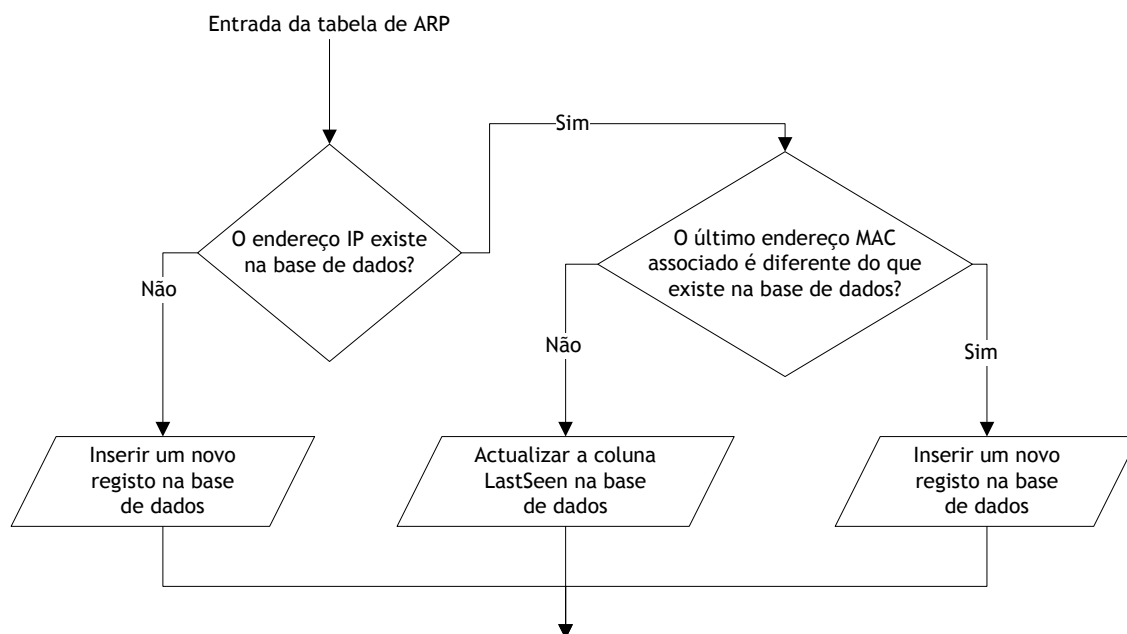


Figura 5.8 - Fluxograma do tratamento de cada entrada da tabela de ARP

5.3.4.3 Recolha da lista de estações associadas

Este módulo tem como principal objectivo fazer o registo das estações associadas a cada SSID e a cada ponto de acesso, permitindo a obtenção de um histórico da movimentação das mesmas. Ao cruzar os dados recolhidos por este módulo e pelo descrito anteriormente torna-se possível saber qual o endereço IP utilizado pela estação ao longo da sua movimentação.

Tal como o módulo anterior, a implementação efectuada também recorre a um script para realizar a operação, utilizando a seguinte tabela no SGBD:

associated_stations	
PK	<u>Device_ID</u>
PK	<u>SSID</u>
PK	<u>MAC_Address</u>
PK	<u>FirstSeen</u>
	LastSeen

Figura 5.9 - Tabela utilizada pelo módulo de recolha da lista de estações associadas

Durante o processo de recolha das estações associadas a cada ponto de acesso, o script sujeita cada associação a um tratamento que segue o seguinte fluxograma.

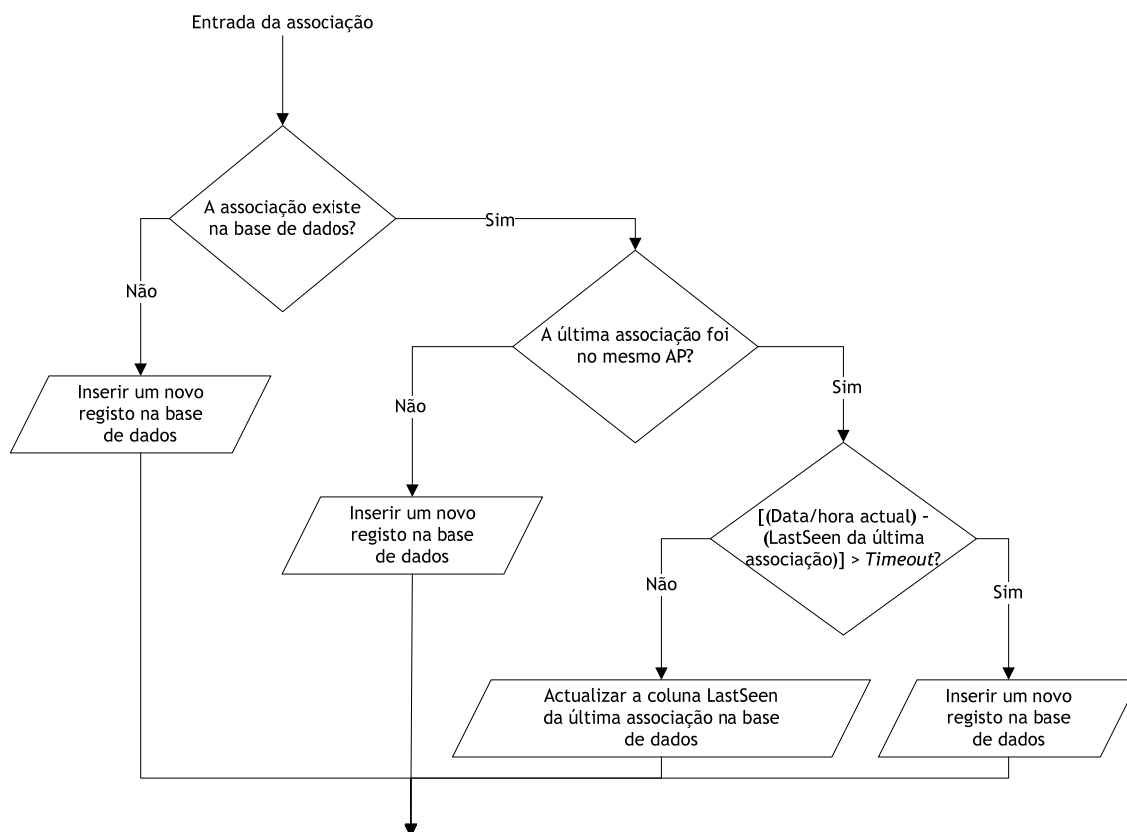


Figura 5.10 - Fluxograma do tratamento de cada associação a um ponto de acesso

5.3.5 Servidor AAA

Nesta solução o servidor AAA é a entidade que fornece os serviços de autenticação, autorização e contabilização para os pontos de acesso. A comunicação entre este e os pontos de acesso é efectuada com recurso ao protocolo RADIUS, através da utilização do pacote de *software* FreeRADIUS.

5.3.5.1 Autenticação e Autorização

O serviço de autenticação e autorização é utilizado quando é necessário um controlo de acessos à rede centralizado, normalmente efectuado com recurso a norma IEEE 802.1X.

Na implementação desenvolvida o *backend* utilizado foi o SGBD MySQL, mas em muitos ambientes empresariais já existe um sistema de directório implantando para vários serviços, podendo ser necessário interligar o servidor AAA a esse sistema de directório. Na maioria dos casos o acesso ao sistema de directório é efectuado utilizando o protocolo LDAP (*Lightweight Directory Access Protocol*), sendo este protocolo bem suportado pelo servidor AAA escolhido.

5.3.5.2 Contabilização

Foi analisada a hipótese de fazer a contabilização através do protocolo SNMP, tentando utilizar alguma tabela que pudesse fornecer essa informação, mas a conclusão retirada foi que não se tornava viável devido às seguintes razões:

- Os pontos de acesso da Cisco possuem na sua MIB proprietária uma tabela que fornece o número de octetos enviados e recebidos por uma estação associada, mas essa informação é eliminada logo que a estação se desassocie do ponto de acesso, não deixando que o sistema de gestão possa recolhê-la antes que seja eliminada, de forma a construir um histórico.
- Muitos dos pontos de acesso nem disponibilizam essa informação.

Devido às razões anteriores na solução desenvolvida optou-se por fazer a contabilização através deste servidor, sendo também a solução adoptada em muitas infra-estruturas de rede Wi-Fi.

Para a contabilização o protocolo RADIUS utiliza o conceito de sessão.

Uma sessão é iniciada quando o ponto de acesso, ou NAS (*Network Access Server*) na nomenclatura do protocolo, começa a fornecer o acesso à rede a uma estação. Essa sessão acaba quando essa estação é desassociada do mesmo ponto de acesso. Um ponto de acesso pode conter várias sessões em simultâneo, cada uma possui um identificador único.

Segue-se um diagrama de sequência que ilustra a troca de mensagens de contabilização entre um ponto de acesso e o servidor AAA.

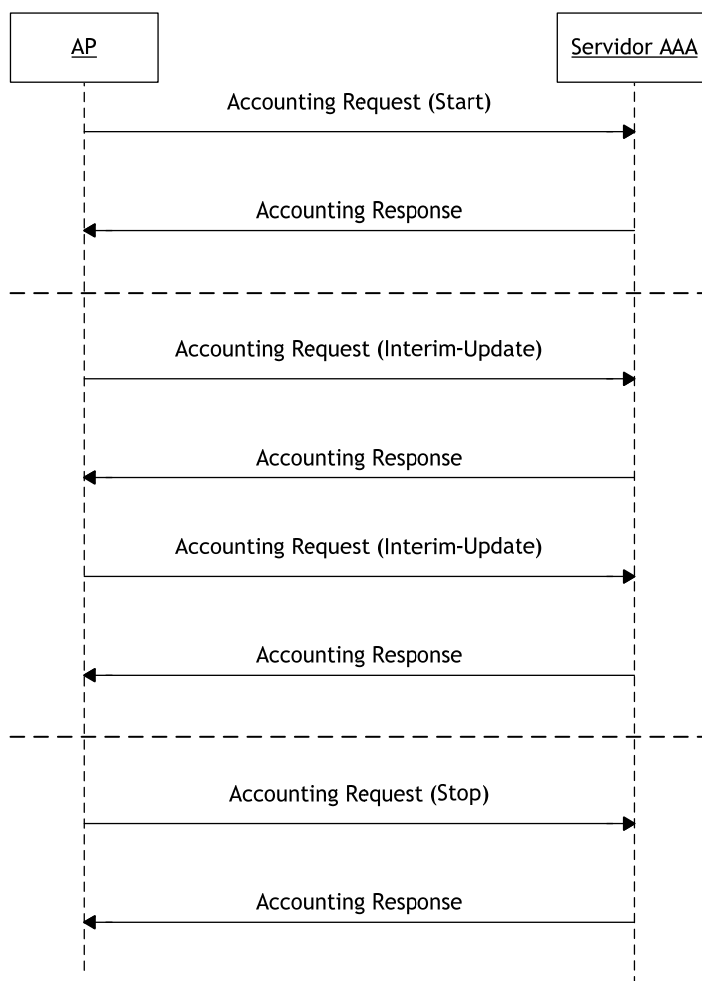


Figura 5.11 - Diagrama de sequência com as mensagens de contabilização do protocolo RADIUS

Para qualquer mensagem recebida pelo servidor é sempre enviada uma confirmação através de uma mensagem de *Accounting Response*, pois o transporte destas mensagens é feito usando o protocolo UDP, onde não é garantida a entrega das mesmas.

Uma sessão começa após a recepção por parte do servidor AAA uma mensagem de *Accounting Request* do tipo *Start*. Nesse momento o servidor AAA insere um novo registo na tabela de contabilização do SGBD.

De uma forma opcional podem ser enviadas, pelo ponto de acesso, mensagens do tipo *Interim-Update*, que permitem actualizar alguns dados da sessão, tais como o número de octetos enviados e recebidos.

A sessão termina quando o servidor AAA receber uma mensagem do tipo *Stop*.

5.3.6 Interface com o Utilizador

O interface com o utilizador é responsável por reunir toda a informação recolhida pelos outros módulos e apresentá-la sob uma forma gráfica. Na implementação desenvolvida este corre numa plataforma *Web*, possibilitando o acesso a partir de qualquer terminal utilizando apenas um *browser*.

De forma a demonstrar o funcionamento do mesmo, seguem-se algumas imagens do interface com o utilizador recolhidas numa pequena rede laboratorial com dois pontos de acesso, Cisco Aironet 1200 e DLink DWL-2100AP, ligados a um *switch* Cisco Catalyst 2960.

5.3.6.1 Equipamentos Geridos

A imagem seguinte mostra a página inicial da aplicação, onde é possível observar um sumário dos equipamentos geridos, assim como o estado de cada um.

The screenshot displays the 'Gestão da Rede' application interface. At the top, there's a navigation bar with tabs for 'Rede', 'Eventos', and 'Utilizadores'. The 'Rede' tab is active. Below the navigation bar, there's a sidebar on the left with a 'Equipamento' section containing 'Listar' and 'Adicionar' links. The main content area is titled 'Rede' and contains a 'Resumo' table showing the count of equipment types: AP (4) and Switch (1). Below this is a table titled 'Equipamentos' listing individual devices with columns for Nome, Endereço, Tipo, Estado, and a link to 'Detalhes Eventos Histórico'.

Gestão da Rede					
Rede					
Equipamento		Rede			
Listar					
Adicionar					
		Resumo			
		Tipo		Quantidade	
		AP		4	
		Switch		1	
		Equipamentos			
		Nome	Endereço	Tipo	Estado
		Cisco AP 1200	172.16.2.18	AP	Online
		gnu-sw3	172.16.2.30	Switch	Online
		teste	192.168.106.1	AP	Offline
		teste	192.168.106.5	AP	Offline
		DLink AP	172.16.2.16	AP	Online
					Detalhes Eventos Histórico

Figura 5.12 - Página inicial da aplicação

Num ambiente de produção uma das melhorias nesta página seria adicionar um diagrama com os equipamentos, contendo alarmes sinópticos que informam o utilizador sobre a existência de eventos não confirmados em cada equipamento.

A solução desenvolvida precisa que lhe sejam introduzidos os dados dos equipamentos para serem monitorizados. Os dados necessários são os seguintes:

- **Nome** - Um nome descritivo do equipamento.
- **Endereço** - Endereço do equipamento, podendo ser um *hostname* ou endereço IP.
- **Tipo** - Ponto de Acesso, *Switch* ou *Router*.
- **Parâmetros SNMP**
 - **Comunidade** - Comunidade SNMP de leitura e escrita do equipamento.
 - **Timeout** - Tempo de espera máximo, em milissegundos, até que o sistema volte a realizar novo pedido.
 - **Tentativas** - Número de tentativas a efectuar, em caso de *timeout*, até afirmar que o sistema se encontra *offline*.
- **Localização** - Campo opcional e apenas informativo com uma descrição da localização do equipamento. Pode ser utilizado para a ordenação do equipamento por localização.
- **Descrição** - Campo opcional para alguma descrição ou comentário que o utilizador ache pertinente.

Este passo é executado numa página como a mostrada na figura seguinte.

The screenshot displays the 'Gestão da Rede' web application interface. At the top, there is a navigation bar with three tabs: 'Rede' (selected), 'Eventos', and 'Utilizadores'. Below the navigation bar, the main content area is titled 'Equipamento' and contains two links: 'Listar' and 'Adicionar'. The 'Adicionar Equipamento' form is visible, featuring several input fields and a dropdown menu. The fields are labeled: 'Nome:', 'Endereço:', 'Comunidade SNMP:', 'Timeout SNMP (ms):' (with a value of 1000), 'Tentativas SNMP:' (with a value of 3), 'Tipo:' (a dropdown menu showing 'AP'), 'Recolher Tabela ARP:' (a checkbox), 'Localização (Opcional):', and 'Descrição (Opcional):'. A 'Adicionar' button is located at the bottom of the form.

Figura 5.13 - Página que permite adicionar equipamento

5.3.6.2 Detalhes do Equipamento

Nesta página são mostrados todos os detalhes disponíveis sobre um dos equipamentos. No caso dos pontos de acesso, para além da informação do próprio sistema e dos interfaces de rede, também é mostrada a informação relacionada com a parte rádio. Essa informação inclui o canal de operação, o débito máximo, a potência de emissão e SSIDs, permitindo ao utilizador alterar qualquer um desses parâmetros. Segue-se uma figura que melhor ilustra as potencialidades.

Gestão da Rede

Rede
Eventos
Utilizadores

Detalhes

Informação presente na Base de Dados

Nome: Cisco AP 1200
Endereço: 172.16.2.18 (172.16.2.18)
Tipo: AP
Comunidade SNMP: private
Localização: Netlab
Descrição: AP de testes CISCO
Recolher Tabela ARP: Sim

Alterar
Remover

Informação do Sistema

Descrição: Cisco IOS Software, C1200 Software (C1200-K9W7-M), Version 12.3(8)JEC, RELEASE SOFTWARE (fc1) Technical Support: <http://www.cisco.com/techsupport> Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Thu 25-Oct-07 22:24 by dchih
Uptime: 1808.51 s

Interfaces de Rede

Interface	Débito Máximo	Estado Administrativo	Estado Operacional	Opções
Dot11Radio0	54 Mb/s	Activo	Activo	Histórico
FastEthernet0	100 Mb/s	Activo	Activo	Histórico
Null0	4294.967295 Mb/s	Activo	Activo	Histórico
BVI1	54 Mb/s	Activo	Activo	Histórico

Dados do Ponto de Acesso

Interface	Canal	Débito Máximo	Potência	SSID(s)
Dot11Radio0	4 (Auto)	54 Mb/s	1 mW	netlab
	1 Alterar	1 Mb/s Alterar	1 mW Alterar	teste

SSIDs

SSID	Difusão do nome	VLAN
netlab	Desactivada	1

Clientes Associados

Número total de clientes associados: 2 [Monitorizar](#)

SSID	Endereço MAC	Débito Máximo	SSI	SNR
netlab	00130290a616	54 Mb/s	-60	37
netlab	0013e83805c7	54 Mb/s	-55	42

Figura 5.14 - Página onde são mostrados os detalhes de um AP

Também é possível visualizar uma lista de estações associadas, com detalhes como nível de sinal e relação sinal/ruído para cada estação.

Num ambiente de produção pode ser útil ter uma página que mostre todos os pontos de acesso e permita efectuar alterações nos vários pontos de acesso em simultâneo, facilitando ao utilizador o processo de alteração.

Tal como na situação anterior, a página de detalhes do equipamento também funciona com outros tipos de equipamentos, tal como *switches* e *routers*. Na figura seguinte é mostrado a página de detalhe de um *switch*.

Gestão da Rede

Rede | Eventos | Utilizadores

Detalhes

Informação presente na Base de Dados

Nome: gnu-sw3
 Endereço: 172.16.2.30 (172.16.2.30)
 Tipo: Switch
 Comunidade SNMP: public
 Localização: Netlab
 Descrição: Switch da Bancada 3
 Recolher Tabela ARP: Sim

[Alterar](#) [Remover](#)

Informação do Sistema

Descrição: Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Sat 05-Jan-08 00:42 by weiliu
Uptime: 2013319.93 s

Interfaces de Rede

Interface	Débito Máximo	Estado Administrativo	Estado Operacional	Opções
Vlan1	1000 Mb/s	Activo	Activo	Histórico
FastEthernet0/1	100 Mb/s	Activo	Activo	Histórico
FastEthernet0/2	100 Mb/s	Activo	Activo	Histórico
FastEthernet0/3	100 Mb/s	Activo	Activo	Histórico
FastEthernet0/4	100 Mb/s	Activo	Inactivo	Histórico
FastEthernet0/5	10 Mb/s	Activo	Inactivo	Histórico
FastEthernet0/6	10 Mb/s	Activo	Inactivo	Histórico
FastEthernet0/7	10 Mb/s	Activo	Inactivo	Histórico
FastEthernet0/8	10 Mb/s	Activo	Inactivo	Histórico
FastEthernet0/9	100 Mb/s	Activo	Activo	Histórico
FastEthernet0/10	10 Mb/s	Activo	Inactivo	Histórico
FastEthernet0/11	100 Mb/s	Activo	Inactivo	Histórico
FastEthernet0/12	10 Mb/s	Activo	Inactivo	Histórico
FastEthernet0/13	100 Mb/s	Activo	Activo	Histórico

Figura 5.15 - Página onde são mostrados os detalhes de um *switch*

5.3.6.3 Visualização de Eventos

O objectivo desta página é poder mostrar os eventos gerados pelos equipamentos e enviados através de notificações SNMP, quer os eventos gerados pelo próprio sistema de monitorização.

Os eventos podem ser filtrados por qualquer um dos seguintes campos:

- Categoria
- Gravidade
- Equipamento

Gestão da Rede

Rede
Eventos
Utilizadores

Eventos

Página 1 de 49

Data/Hora	Categoria	Gravidade	Equipamento	Mensagem
2008-06-13 15:29:17	Cisco Configuration Management	Normal	Cisco AP 1200 (172.16.2.18)	Configuration Management Event from '1', using '3' to '2'
2008-06-13 15:27:25	IEEE802dot11	Normal	Cisco AP 1200 (172.16.2.18)	Wi-Fi Station "00 1C BF 37 15 FE " deauthenticated
2008-06-13 15:27:24	IEEE802dot11	Normal	Cisco AP 1200 (172.16.2.18)	Wi-Fi Station "00 1C BF 37 15 FE " deauthenticated
2008-06-13 15:27:24	Cisco SysLog	Normal	Cisco AP 1200 (172.16.2.18)	"Interface Dot11Radio0, changed state to down"
2008-06-13 15:27:24	Cisco SysLog	Normal	Cisco AP 1200 (172.16.2.18)	"Interface Dot11Radio0, changed state to up"
2008-06-13 15:17:31	IEEE802dot11	Normal	Cisco AP 1200 (172.16.2.18)	Wi-Fi Station "00 1C BF 37 15 FE " deauthenticated
2008-06-13 15:17:31	IEEE802dot11	Normal	Cisco AP 1200 (172.16.2.18)	Wi-Fi Station "00 1C BF 37 15 FE " deauthenticated
2008-06-13 15:17:30	IEEE802dot11	Normal	Cisco AP 1200 (172.16.2.18)	Wi-Fi Station "00 1C BF 37 15 FE " deauthenticated
2008-06-13 15:17:30	Cisco SysLog	Normal	Cisco AP 1200 (172.16.2.18)	"Interface Dot11Radio0, changed state to down"
2008-06-13 15:17:30	Cisco SysLog	Normal	Cisco AP 1200 (172.16.2.18)	"Interface Dot11Radio0, changed state to up"
2008-06-13 15:17:30	Cisco Configuration Management	Normal	Cisco AP 1200 (172.16.2.18)	Configuration Management Event from '2', using '3' to '4'
2008-06-13 15:17:29	Cisco SysLog	Normal	Cisco AP 1200 (172.16.2.18)	"Packet to client 001c.bf37.15fe reached max retries, removing the client"
2008-06-13 04:39:15	Cisco Configuration Management	Normal	Cisco AP 1200 (172.16.2.18)	Configuration Management Event from '1', using '3' to '2'
2008-06-13 04:39:03	Cisco Configuration Management	Normal	Cisco AP 1200 (172.16.2.18)	Configuration Management Event from '1', using '2' to '3'
2008-06-13 04:38:57	Cisco Configuration Management	Normal	Cisco AP 1200 (172.16.2.18)	Configuration Management Event from '1', using '3' to '2'
2008-06-13 04:36:57	Cisco Configuration Management	Normal	Cisco AP 1200 (172.16.2.18)	Configuration Management Event from '1', using '3' to '2'
2008-06-13 04:36:54	Cisco Configuration Management	Normal	Cisco AP 1200 (172.16.2.18)	Configuration Management Event from '1', using '3' to '4'
2008-06-13			Cisco AP 1200	Configuration Management Event from

Figura 5.16 - Página onde é possível visualizar um histórico de eventos

5.3.6.4 Histórico de valores do equipamento

Esta página permite que sejam visualizados vários parâmetros de cada equipamento sob uma forma gráfica. Também é possível visualizar os valores mínimos e máximos desses mesmos parâmetros, assim como a sua evolução ao longo de uma semana, mês ou ano.

A figura seguinte apresenta um exemplo onde é possível observar o histórico do canal utilizado, número de estações associadas e o tráfego de um interface rádio de um ponto de acesso.

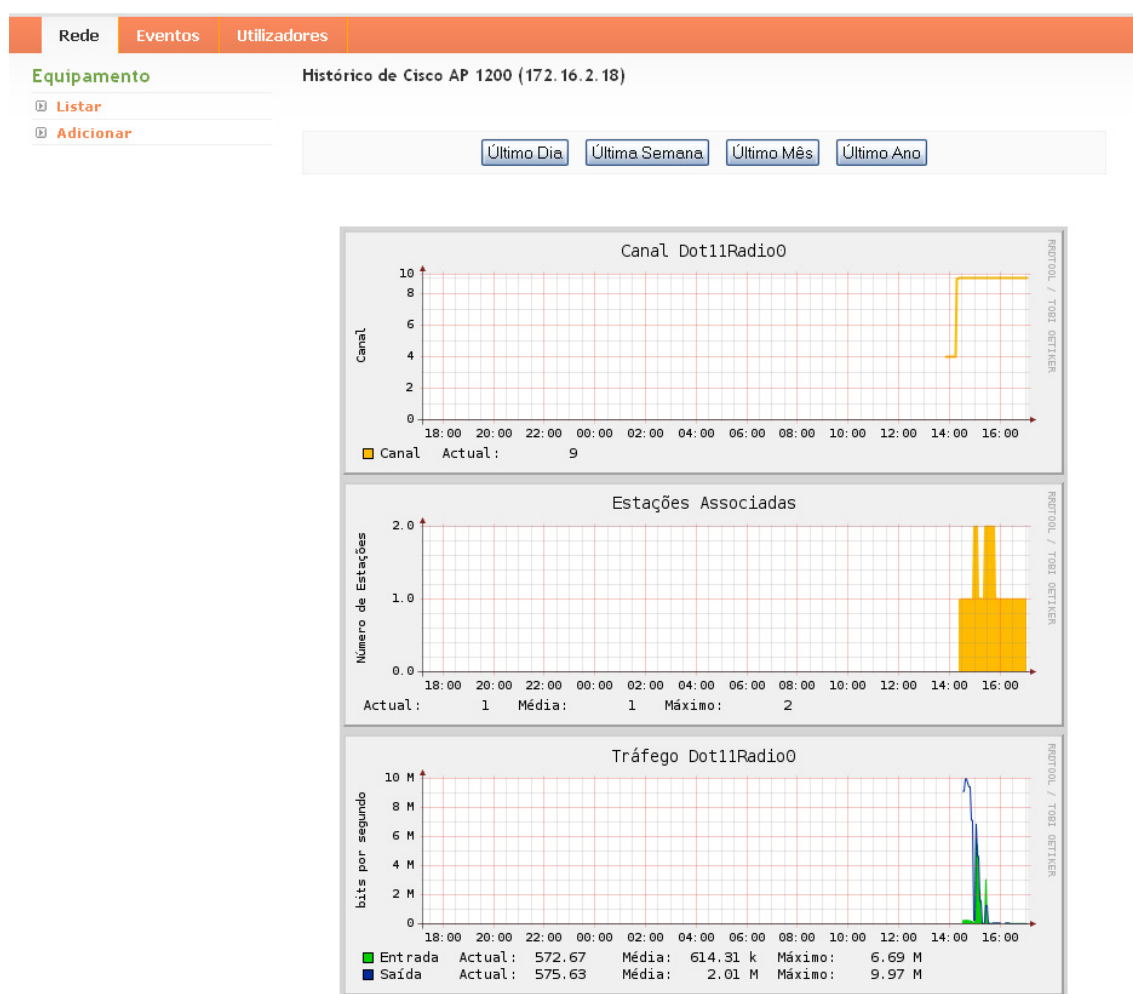


Figura 5.17 - Página onde é possível observar o histórico de várias leituras de um AP

5.3.6.5 Pesquisa de Estações

Esta página foi concebida para permitir a pesquisa de estações pelo seu endereço MAC, ou pelo endereço IP utilizado num determinado momento, sendo possível determinar em que ponto de acesso a estação esteve ligada, assim como o SSID que esteve associada.

Na imagem seguinte é mostrado um exemplo de uma pesquisa.



AP	SSID	Endereço MAC	Endereço IP	Data/Hora Inicio	Data/Hora Fim
Cisco AP 1200	netlab	0013e83805c7	169.254.10.1	2008-06-27 16:30:00	2008-06-27 16:55:00
Cisco AP 1200	netlab	0013e83805c7	172.16.2.119	2008-06-27 15:00:00	2008-06-27 16:25:00

Figura 5.18 - Página que contém o histórico da movimentação de uma estação

Na figura anterior é notória a alteração do endereço IP da estação, tendo o mesmo acontecido devido a uma falha ocorrida no servidor de DHCP. A estação, a correr o sistema operativo Windows, tentou renovar o seu endereço de IP e como não obteve resposta do servidor de DHCP, atribuiu automaticamente um endereço IP 169.X.X.X, tal como é habitual neste sistema operativo.

5.3.6.6 Contabilização

Estas páginas foram desenvolvidas de forma a realizarem uma das ligações entre o sistema AAA e o sistema de gestão, mostrando a contabilização efectuada pelos pontos de acesso.

Na figura seguinte é mostrada a página onde é possível observar o consumo total de cada utilizador, assim como o tempo total que cada utilizador esteve ligado à rede.

Gestão da Rede

Rede | Eventos | **Utilizadores**

Opções

- ☒ Pesquisa de Estações

RADIUS

- ☒ Autorizações
- ☒ **Contabilização**

Contabilização

Username:

Username	Tempo Total (s)	Tráfego Total de Entrada (KB)	Tráfego Total de Saída (KB)
salgado	15560	664130	20073
filipe	8720	73569	2537756
nuno	56821	1120	20
ee03058@fe.up.pt	6895	711	3429

Figura 5.19 - Página onde é possível observar os consumos de todos os utilizadores

Também é possível detalhar a contabilização de tráfego de cada utilizador, mostrando o tempo dispendido em cada sessão assim como o tráfego consumido em cada sessão, tal como é representado na figura seguinte.

Gestão da Rede

Rede | Eventos | **Utilizadores**

Opções

- ☒ Pesquisa de Estações

RADIUS

- ☒ Autorizações
- ☒ **Contabilização**

Contabilização

Username:

Username	Endereço MAC	Sessão				Tráfego Total de Entrada (KB)	Tráfego Total de Saída (KB)
		Data/Hora Início	Data/Hora Fim	Tempo (s)			
filipe	0013.0290.a616	2008-06-27 14:21:37	2008-06-27 15:53:24	5508	68560	2493183	
filipe	001c.bf37.15fe	2008-06-13 15:17:31	2008-06-13 15:27:24	593	816	5048	
filipe	001c.bf37.15fe	2008-06-13 04:39:20	2008-06-13 15:17:29	2531	4184	39522	
filipe	001c.bf37.15fe	2008-06-13 04:37:32	2008-06-13 04:39:00	88	7	2	

Figura 5.20 - Página onde é possível visualizar os detalhes das várias sessões de um utilizador

5.4 Segurança da solução

A comunicação entre o sistema de gestão e os equipamentos é efectuada com recurso a três diferentes protocolos. Segue-se uma análise à sua segurança e algumas recomendações com o objectivo de minimizar as suas falhas de segurança.

5.4.1 Protocolo SNMP

Devido à fraca implantação da terceira versão do protocolo SNMP, a solução foi implementada com recurso à segunda versão do protocolo (SNMPv2c). Nesta versão do protocolo o único mecanismo de segurança existente é o nome de comunidade (*community string*), que apenas permite a validação do acesso ao agente SNMP do equipamento. A informação contida nos pacotes trocados entre os agentes SNMP presentes nos equipamentos e a estação de gestão não sofre qualquer processo de encriptação.

O acesso indevido a esta informação pode levantar alguns problemas pois sabendo o nome de comunidade de escrita de um equipamento possibilita que sejam alteradas as suas configurações, podendo levar à indisponibilidade da infra-estrutura de rede.

Este problema, embora não possa ser totalmente resolvido usando o protocolo SNMPv2, pode ser minimizado através da utilização das seguintes recomendações:

- Utilização de uma VLAN específica para as comunicações entre o sistema de gestão e os agentes SNMP, permitindo uma maior separação entre o tráfego das estações cliente e o tráfego de gestão da rede.
- Utilização de listas de controlo de acessos nos equipamentos para limitar o acesso aos agentes SNMP, permitindo o acesso apenas ao endereço da estação de gestão.
- Utilização de nomes de comunidade SNMP não triviais. A maioria dos fabricantes adopta o nome de comunidade `public` para acesso de leitura e `private` para o acesso de leitura e escrita. Estes nomes não deverão ser utilizados num ambiente de produção pois são demasiado vulgares.

5.4.2 Protocolo Telnet

O acesso ao terminal dos equipamentos embora tenha sido efectuado com recurso ao protocolo telnet nos testes, num ambiente de produção deverá ser efectuado com recurso ao protocolo SSH. Este último possibilita uma autenticação mais segura assim como a confidencialidade das comunicações, ao contrário do protocolo telnet. Tal como no protocolo analisado no ponto anterior o acesso indevido aos dados de autenticação transportados de

forma aberta no protocolo telnet pode ser uma falha grave na segurança da infra-estrutura de rede.

De forma a minimizar a falha de segurança do protocolo devem ser seguidas as seguintes recomendações:

- Deve ser dada a preferência ao protocolo SSH, caso o equipamento suporte.
- Utilização de uma VLAN específica para estas comunicações, permitindo uma maior separação entre o tráfego das estações cliente e este tráfego.
- Utilização de listas de controlo de acessos nos equipamentos para limitar o acesso ao terminal a apenas aos endereços da rede de gestão.

5.4.3 Protocolo RADIUS

O protocolo RADIUS foi desenvolvido de raiz para fornecer um serviço de autenticação, daí já ter incluído alguns mecanismos de segurança. Embora existam várias vulnerabilidades relacionadas com a sua segurança, essas falhas não comprometem directamente a segurança dos equipamentos da infra-estrutura. No entanto as recomendações são:

- Tal como nos protocolos analisados anteriormente é recomendável a utilização de uma VLAN específica para as comunicações entre os pontos de acesso e o servidor RADIUS.
- Recorrer a chaves partilhadas (entre os pontos de acesso e o servidor RADIUS) complexas.

Capítulo 6

Conclusões

Este último capítulo apresenta uma síntese do trabalho reportado neste documento, referindo as conclusões retidas. São também apresentadas as perspectivas de desenvolvimento futuro.

6.1 Síntese do trabalho desenvolvido

O trabalho desenvolvido culminou na implementação de um protótipo de uma plataforma de gestão integrada de uma infra-estrutura de rede Wi-Fi com recurso ao protocolo SNMP. A primeira parte do trabalho centrou-se na realização de um estudo inicial sobre o funcionamento das redes Wi-Fi e do protocolo SNMP, de forma a perceber as suas potencialidades e limitações.

De seguida foram definidos os requisitos para uma plataforma deste tipo a partir de alguns dos problemas de gestão e operação encontrados neste tipo de infra-estruturas de rede.

Após a delineação dos requisitos, foram analisadas algumas MIBs com o objectivo de determinar quais as informações que seriam possíveis de obter através do protocolo SNMP, assim como determinar qual o procedimento de alteração de objectos de forma a possibilitar a alteração de configurações dos equipamentos. Esta análise permitiu obter a seguinte conclusão que foi determinante para o desenvolvimento da arquitectura da solução:

Não existe uniformização dos objectos de gestão relacionados com a norma IEEE 802.11, entre os vários fabricantes, obrigando a que sejam utilizados os objectos de MIBs proprietárias.

A anterior conclusão levou a que tivesse que ser desenvolvida para a plataforma uma camada de abstracção do *hardware* de forma a suportar diferentes fabricantes com o mínimo de alterações.

Por último foi efectuada a implementação do protótipo, comprovando que é possível efectuar a gestão de uma infra-estrutura deste tipo com recurso ao protocolo SNMP, embora não de uma forma homogénea, para os diferentes fabricantes, como seria desejável.

6.2 Desenvolvimento futuro

O trabalho realizado apresenta uma implementação de um protótipo de uma plataforma de gestão integrada de uma infra-estrutura de rede Wi-Fi relativamente simples, que pode ser enriquecida pela inclusão das seguintes funcionalidades:

- Descoberta automática do equipamento - Esta funcionalidade permite facilitar a integração da solução numa infra-estrutura de rede já existente, pois elimina o tempo dispendido a adicionar o equipamento.
- Módulo de *site survey* que permita analisar com detalhe a cobertura da infra-estrutura e a possível interferência entre pontos de acesso adjacentes, facilitando o processo de escolha da potência de emissão e do canal de operação de cada ponto de acesso. Também se torna importante na fase de planeamento de uma expansão da infra-estrutura, pois permite a escolha dos locais para serem colocados os pontos de acesso, maximizando a cobertura da rede.
- Possibilidade de monitorizar a qualidade do sinal recebido pelas estações através de sondas colocadas no local. Para além de melhorar o diagnóstico, permite, de uma forma adicional, detectar estações e/ou pontos de acesso interferentes.

Referências

- [1]. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. [IEEE Standard 802.11]. 1999.
- [2]. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. [IEEE Standard 802.11b]. 1999.
- [3]. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band. [IEEE Standard 802.11a]. 1999.
- [4]. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. [IEEE Standard 802.11g]. 2003.
- [5]. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. [IEEE Standard 802.11i]. 2004.
- [6]. Port-Based Network Access Control. [IEEE Standard 802.1X]. 2004.
- [7]. **Rose, M. and McCloghrie, K.** Structure and Identification of Management Information for TCP/IP-based Internets. [RFC-1155]. 1990.
- [8]. **McCloghrie, K., Perkins, D. and Schoenwaelder, J.** Structure of Management Information Version 2 (SMIv2). [RFC-2578]. 1999.
- [9]. **McCloghrie, K. and Rose, M.** Management Information Base for Network Management of TCP/IP-based internets:MIB-II. [RFC-1213]. 1999.
- [10]. Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework. [ISO 7498-4]. 1989.

- [11]. CiscoWorks Wireless LAN Solution Engine (WLSE). [Online]
<http://www.cisco.com/en/US/products/sw/cscowork/ps3915/>.
- [12]. Proxim Wireless - ProximVision. [Online]
<http://www.proxim.com/products/proximvision/index.html>.
- [13]. Motorola RF Management Software. [Online]
<http://www.motorola.com/business/v/index.jsp?vgnextoid=7c1de90e3ae95110VgnVCM1000008406b00aRCRD&vgnnextchannel=802d3acf35e95110VgnVCM1000008406b00aRCRD>.
- [14]. Tobi Oetiker's MRTG - The Multi Router Traffic Grapher. [Online]
<http://oss.oetiker.ch/mrtg/>.
- [15]. Cacti: The Complete RRDTool-based Graphing Solution. [Online]
<http://www.cacti.net/>.
- [16]. *AirWave - Wireless Network Management Software for WiFi, Mesh, WiMAX and more.* [Online] <http://www.airwave.com/products/AMP/>.
- [17]. *ManageEngine WiFi Manager: Wireless LAN Security and Management.* [Online]
<http://manageengine.adventnet.com/products/wifi-manager/index.html>.
- [18]. Stallings, William. *SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*. 3rd Edition. s.l. : Addison Wesley, 1999. ISBN 0-20-148534-6.
- [19]. McCloghrie, K., Perkins, D. and Schoenwaelder, J. Textual Conventions for SMIv2. [RFC-2579]. 1999.
- [20]. McCloghrie, K. and Rose, M. Management Information Base for network management of TCP/IP-based internets. [RFC-1156]. 1990.
- [21]. Mauro, Douglas R and Schmidt, Kevin J. *Essential SNMP*. 2nd Edition. s.l. : O'Reilly, 2005. ISBN 0-59-600840-6.
- [22]. *Network management system for wireless LAN service.* Jeon, Boo-Sun, Ko, Eun-Jin and Lee, Gil-Haeng. 2003. 10th International Conference on Telecommunications. Vol. 2, pp. 948-953. ISBN 0-78-037661-7.
- [23]. Henry, Paul S and Luo, Hui. WiFi: what's next? *IEEE Communications Magazine*. Dezembro 2002, Vol. 40, 12, pp. 66-72.
- [24]. Crow, Brian P., et al. IEEE 802.11 Wireless Local Area Networks. *IEEE Communications Magazine*. September 1997, Vol. 35, 9, pp. 116-126.

[25]. Case, J., et al. Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2). [RFC-1906]. 1996.

[26]. —. Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2). [RFC-1905]. 1996.

[27]. Case, J, et al. A Simple Network Management Protocol (SNMP). [RFC-1157]. 1990.

[28]. *SNMP Research International, Inc.* [Online] <http://www.snmp.com/>.

[29]. *Net-SNMP*. [Online] <http://net-snmp.sourceforge.net/>.