Arquitecturas e Ferramentas para Gestão de Redes e Sistemas
Estudo de um Caso

Nuno Filipe de Oliveira Lima Rodrigues Carvalho

Dissertação para obtenção do Grau de Mestre em

Engenharia Informática

Área de Especialização em

Arquitecturas, Sistemas e Redes

Orientador: Maria João Viamonte

Porto, Outubro de 2009

AGRADECIMENTOS

No fim de um ciclo académico, longo e exigente, bem como proveitoso e compensador, não podia deixá-lo acabar sem o devido agradecimento a todos que com paciência, empenho e dedicação foram facilitando o meu percurso de alguns anos por esta instituição de ensino que me formou e que muito prezo.

Aos meus colegas e professores, que o tempo decidiu que se tornassem amigos, pela tolerância, compreensão e pela relação pessoal que criámos e que espero que nunca se perca.

Aos meus orientadores desta caminhada, Doutor António Costa, Eng. Jorge Pinto Leite e Doutora Maria João Viamonte, que mais que nenhuns outros, passaram a fazer parte da minha vida, tanto pelos conhecimentos técnicos transmitidos, como pela entrega e cumplicidade que se criou ao longo destes anos.

RESUMO

O presente trabalho teve como objectivo o estudo de soluções para a gestão de redes e sistemas, tendo por base o actual crescimento e desenvolvimento das tecnologias de informação. A constante evolução cria novas necessidades de monitorização e obriga a procurar ferramentas adequadas para apoio à decisão e gestão.

O sistema de informação de uma organização é primordial ao desenvolvimento da actividade de negócio, tendo por isso de estar sempre funcional e ao melhor nível em termos de desempenho.

Analisar os modelos de gestão e ferramentas disponíveis é o primeiro passo para uma escolha acertada. No entanto, também é necessário possuir um conhecimento profundo da configuração da infra-estrutura e da orgânica da instituição e das tecnologias envolvidas. O estudo efectuado terminou com a implementação de um sistema de gestão adequado a um cenário real, bastante rico na diversidade de tecnologias e sistemas.

PALAVRAS-CHAVE

Gestão de Redes, Falhas, Configuração, Utilização, Desempenho, Segurança, SNMP.

ABSTRACT

This project was designed to study solutions for managing networks and systems, based on the current growth and development of information technology.

The constant evolution carries out new monitoring needs and finding the most adequate tools for decision support and management is crucial.

The information system of an organization is paramount to the development of the core business, and therefore should always be functional and at the best performance level.

Analyzing management models and available tools is the first step to the right choice. On the other hand, there is the need to know the technologies involved, the configuration of the substructure and the organization of the institution.

The study carried out, has triggered the adoption of a solution that was configured and adapted to the reality of the company, which is very rich concerning diversity of technology and systems available.

KEYWORDS

Network Managment, Fault, Configuration, Accounting, Performance, Security and SNMP

ÍNDICE

Agradecimentos 2
Resumo 3
Palavras-chave 3
Abstract 4
Keywords 4
Índice 5
Lista Figuras 8
Lista Tabelas 9
1. Introdução 10
1.1. Enquadramento Temático 10
1.2. Objectivos 11
1.3. Estrutura 11
2. Arquitecturas de Gestão de Redes 12
2.1. Introdução 12
2.2. Modelos de Gestão de Redes 12
2.2.1. Modelo OSI 13
2.2.2. Modelo TCP/IP 15
2.2.3. Modelo TMN 17
2.2.4. Modelo de Gestão SNMP 19
2.2.5. Arquitectura do Modelo de Gestão TCP/IP 20
2.2.6. Remote Network Monitoring (RMON) MIB 25
2.3. Modelos de Gestão de Sistemas 28
2.3.1. DMI – Desktop Management Interface 28
2.3.2. CIM – Common Information Model 30
2.3.3. JMX – Java Management eXtensions 31
2.3.4. WBEM - Web Based Enterprise Management 32
3. Plataformas de Gestão 34
3.1. Introdução 34
3.2. Requisitos Plataforma de Gestão 34
3.3. Plataformas de Gestão Generalistas 36
3.3.1. HP OpenView 36
3.3.2. IBM Tivoli NetView 38
3.3.3. Microsoft System Center Configuration Manager 39
3.3.4. OpenNMS 41
3.3.5. Landesk Management Suite 43

3.3.6. Spiceworks ... 45
3.4. Análise Comparativa ... 46
4. Estudo de um Caso ... 49
4.1. Introdução ... 49
4.2. A RTP - Rádio e Televisão de Portugal ... 49
4.3. O Sistema de Informação Actual ... 49
4.3.1. Sistemas ... 50
4.3.2. A Infra-estrutura de Comunicações de Dados ... 51
4.3.3. Monitorização Actual ... 52
4.3.4. Requisitos da Solução ... 53
4.3.5. Monitorização ... 54
4.3.6. Gestão de Actualizações ... 55
4.3.7. Gestão de Activos de Rede ... 56
5. Implementação de uma Solução ... 58
5.1. Introdução ... 58
5.2. A Plataforma OpenNMS ... 58
5.2.1. As Funções de Gestão OpenNMS ... 59
5.2.2. Preparação / Instalação ... 60
5.2.3. Configuração ... 60
5.2.4. Configuração Auto Discover ... 62
5.2.5. Monitorização SNMP ... 63
5.2.6. Alertas por Eventos ... 67
5.2.7. Definição de Grupos de Dispositivos ... 71
5.2.8. Definição de Tempos de Manutenção ... 72
5.2.9. Relatórios ... 73
5.3. Gestão de Actualizações ... 76
5.4. Gestão de Activos de Rede ... 76
5.5. Resultados ... 77
5.5.1. Monitorização ... 77
5.5.2. Alertas por Eventos ... 78
5.5.3. Gestão de Actualizações ... 78
5.5.4. Gestão de Activos de Rede ... 79
6. Conclusões ... 80
6.1. Introdução ... 80
6.2. SÍntese ... 80
6.3. Conclusões ... 80
6.4. Trabalho Futuro ... 81

6.4.1. Melhoramentos na Aplicação Prática do Modelo 81
6.4.1. Áreas de Investigação Futura 82
1. Acrónimos 83
2. Referências 85

LISTA FIGURAS

Figura 2.1 - Modelo OSI 13
Figura 2.2 - Modelo TCP/IP 16
Figura 2.3 - Modelo OSI e Modelo TCP/IP 17
Figura 2.4 - Modelo TMN 18
Figura 2.5 - Sistema de Gestão SNMP 20
Figura 2.6 - Excerto de uma MIB 21
Figura 2.7 - Funcionamento Mensagens SNMP 22
Figura 2.8 - Arquitectura protocolar do SNMPv3 23
Figura 2.9 - Entidade SNMP 24
Figura 2.10 - RMON 25
Figura 2.11 - Modelo OSI e Implementação RMON 26
Figura 2.12 - MIB RMON v1 27
Figura 2.13 - MIB RMON v2 28
Figura 2.14 - Desktop Management Interface 30
Figura 2.15 - Common Information Model 31
Figura 2.16 - Arquitectura JMX 32
Figura 2.17 - WBEM 33
Figura 3.1 - HP OpenView 36
Figura 3.2 - IBM Tivoli NetView 39
Figura 3.3 - Microsoft System Center Configuration Manager 40
Figura 3.4 - OpenNMS 41
Figura 3.5 - OpenNMS - Exemplo Gráfico 43
Figura 3.6 - Landesk Management Suite 44
Figura 3.7 - Spiceworks 45
Figura 4.1 - Esquema de Rede Dados (CNA) 51
Figura 4.2 - Cisco Network Assistant 57
Figura 5.1 - OpenNMS – Login 61
Figura 5.2 - OpenNMS - Config Auto Discovery 62
Figura 5.3 - Ficheiro discovery-configuration.xml 63
Figura 5.4 - OpenNMS - Configuração SNMP 64
Figura 5.5 - Ficheiro snmp-config.xml 64
Figura 5.6 - Ficheiro capsd-configuration.xml 65
Figura 5.7 - Exemplos informação SNMP 66
Figura 5.8 - Ficheiro javamail-configuration.properties 67
Figura 5.9 - Configuração destinatários alertas 68

Figura 5.10 - Ficheiro destinationPaths.xml 68
Figura 5.11 - Criação Alerta: Escolha evento 69
Figura 5.12 - Criação Alerta: Definição de Filtros 70
Figura 5.13 - Criação Alerta: Definição do mail 71
Figura 5.14 - Definição de grupos de dispositivos 72
Figura 5.15 - Comunicado Interno 72
Figura 5.16 - Definição tempo de manutenção 73
Figura 5.17 - Gráfico Temperatura Cisco 74
Figura 5.18 - Gráfico Páginas impressas 75
Figura 5.19 - Exemplo Relatório disponibilidade mês anterior 76

LISTA TABELAS

Tabela 3.1 - Análise Sistemas de Gestão 35
Tabela 3.2 - Comparativo Sistemas de Gestão 47
Tabela 4.1 - Sistema de Informação Actual 50
Tabela 4.2 - Monitorização 55

1. INTRODUÇÃO

A massificação da utilização das tecnologias de informação e da Internet para os mais variados fins, e nas mais diversas áreas, levantou problemas de gestão das infra-estruturas de informática, ímpares até ao momento.

Paralelamente o aumento do grau de complexidade das redes e do seu tamanho exige o emprego de um sistema de gestão que proporcione qualidade de serviço, proactividade, diferenciação de tráfego e o suporte multifacetado de serviços, assim como integração com o processo de serviços e negócio.

Esta realidade obriga à construção de mecanismos e normas de gestão mais ricos nas suas funcionalidades e adaptados aos novos cenários.

Nos próximos Capítulos, o leitor terá a oportunidade de tomar conhecimento de que uma gestão efectiva terá de ser baseada no conhecimento profundo dos mecanismos de gestão, das tecnologias envolvidas, da configuração da infra-estrutura e da orgânica da instituição. O estudo efectuado culminou com a implementação prática de um sistema de gestão adequado a um cenário real, bastante rico na diversidade de tecnologias e sistemas.

1.1. ENQUADRAMENTO TEMÁTICO

O alargamento das redes, o aumento da sua complexidade e a heterogeneidade dos equipamentos a elas ligados têm dificultado de uma forma geral a sua gestão e monitorização. Garantir uma determinada qualidade de serviço fim-a-fim, ou disponibilizar de uma forma controlada serviços de valor para suportar processos de negócio críticos, são objectivos complexos a que a área da gestão de redes tem tentado dar resposta.

As plataformas de gestão disponíveis oferecem um conjunto de recursos básicos para o desenvolvimento de aplicações de gestão. As soluções de gestão prontas, do tipo "*Plug and Play*", oferecidas por estas plataformas são poucas e restritas. Pelo que, para atender às reais necessidades das empresas, as soluções criadas devem ser personalizadas.

No entanto, a gestão e monitorização das redes, de uma forma ou de outra executadas pelos seus administradores, mas evidenciando uma clara falta de integração. Geralmente os administradores vêem-se obrigados a gerir uma amálgama de equipamentos baseados em diferentes tecnologias, obrigando a controlar vários domínios de conhecimento diferentes, em áreas tão distintas como a gestão de um sistema operativo de rede, ou a configuração de um *router* e frequentemente sem qualquer tipo de integração. Assim, o interesse em uniformizar a gestão destes recursos, é claramente importante permitindo definir a um nível de abstracção superior, a implementação de políticas concertadas que estabeleçam as regras básicas de funcionamento da infra-estrutura. Só assim se poderá adequar a infra-estrutura às necessidades da instituição, implementando os mecanismos e procedimentos de gestão, necessários ao garante efectivo dos serviços.

1.2. OBJECTIVOS

Com este trabalho pretende-se estabelecer uma série de requisitos, estudar e identificar as soluções de mercado que melhor lhes respondem, proceder à sua implementação e analisar o resultado da aplicabilidade da solução encontrada a um cenário real, no caso, a infra-estrutura de informática da RTP Porto.

1.3. ESTRUTURA

O documento escrito está organizado em 6 principais capítulos desde o seu enquadramento, passando pelos conceitos teóricos e técnicos fundamentais, pelos detalhes das contribuições científicas, até às sugestões de trabalho futuro.
Os seis capítulos indicados são:

1. Introdução: Pretende contextualizar o trabalho, delinear os principais objectivos e salientar as contribuições científicas do trabalho realizado.

2. Arquitecturas de Gestão de Redes: Estuda as arquitecturas de gestão e o contexto onde são aplicáveis. São ainda analisadas as funções associadas à gestão de sistemas, que pelas suas particularidades e exigências, conduziu ao desenvolvimento de modelos próprios, pelo que neste capítulo são também descritos alguns destes modelos.

3. Plataformas de Gestão: São analisadas as características principais de uma plataforma de gestão e estudadas as principais plataformas de gestão disponíveis no mercado. Com este estudo pretende-se identificar as principais qualidades e deficiências de cada uma delas.

4. Estudo de um caso: Neste capítulo é caracterizada a organização em questão, a Rádio e Televisão de Portugal do Norte – RTP, e a sua infra-estrutura informática, assim como são enumeradas as reais necessidades de gestão da infra-estrutura em estudo.

5. Modelo Proposto – Aplicação: É apresentado o modelo de gestão proposto para o caso particular, assim como é descrita, com algum pormenor, a aplicação de gestão seleccionada para constituir a plataforma de gestão.

6. Conclusões – É feita uma síntese do trabalho realizado, avaliam-se as respectivas contribuições e apontam-se sugestões para trabalho futuro com vista a melhorar e complementar as funcionalidades da plataforma de gestão.

2. ARQUITECTURAS DE GESTÃO DE REDES

2.1. INTRODUÇÃO

As redes informáticas estão nos dias de hoje, presente em qualquer lugar. Desde redes com ou sem fios, de 100MBps até 10GBps, e nas mais variadas formas de transmissão de dados.

Sendo as redes informáticas um factor primordial para a transmissão de dados gerados informaticamente, temos vindo a assistir nas ultimas décadas a uma evolução constante e rápida.

Se a interligação de dois computadores já é considerada uma rede de computadores, onde se pode partilhar serviços, ficheiros, impressoras, etc., hoje em dia assiste-se à massificação e ao crescimento do número de nós nas redes, bem como ao número de serviços partilhados.

A maior exemplificação é a Internet, a rede das redes, à qual estamos hoje em dia, praticamente todos ligados. As formas de "comunicar" através destas novas redes computacionais, são inovadas todos os dias, novos métodos, novas linguagens, novas regras, tendo sempre como objectivo a facilidade, a comodidade e a velocidade proporcionadas. No entanto, esta constante revolução tem de ser acompanhada, monitorizada e gerida.

A análise e resolução dos problemas de gestão podem ter várias aproximações que vão desde o tratamento dos problemas de uma forma isolada até a uma visão integrada da infra-estrutura, actuando sobre ela como um todo. É precisamente nesta última abordagem que as arquitecturas de gestão têm um papel primordial, uma vez que permitem o desenvolvimento de sistemas de gestão abertos, aplicáveis a ambientes heterogéneos existentes nas actuais infra-estruturas informáticas.

Neste capítulo serão abordadas as arquitecturas de gestão e o contexto onde são aplicáveis.

2.2. MODELOS DE GESTÃO DE REDES

Seja qual (ou quais) os modelos de Gestão de redes a seleccionar o objectivo subjacente é sempre o mesmo. Trata-se, de uma forma genérica, de garantir o bom funcionamento da rede e respectivos nós a ela associados, directa ou indirectamente.

Para atingir este objectivo, que aparenta ser simples, é necessário ter em consideração diversos factores e garantir a execução de diversas tarefas, que não podem nunca ser descuidadas.

A gestão encontra-se, conceptualmente, dividida em áreas funcionais, que podem ou não estar todas incluídas no mesmo sistema de gestão.

Para melhor definir o âmbito de Gestão de Redes a *International Organization for Standardization* (ISO) propôs cinco áreas funcionais de actuação: Gestão de Falhas (*Fault*); Gestão de Configuração (*Configuration*); Gestão de Contabilidade de Utilização (*Accounting*); Gestão de Desempenho (*Performance*); e Gestão de Segurança (*Security*). Estas áreas funcionais são normalmente designadas por FCAPS.

As áreas funcionais são endereçadas pelos dois modelos de gestão, o modelo OSI e o modelo TCP/IP.

A Gestão de Falhas é responsável por detectar falhas, ou sintomas de falha e desencadear medidas correctivas.

A Gestão de Configuração é um trabalho permanente de forma a garantir que a rede se encontra em funcionamento, assim como optimizar o desempenho da mesma à medida que as condições ou necessidades vão mudando.

A Gestão de Contabilidade e Utilização tem como objectivo registar a utilização dos recursos.

A Gestão de Desempenho é composta por duas grandes categorias: Monitorização da rede, acção de verificar as actividades da rede para detecção de potenciais problemas de desempenho; e o Controlo da rede, para melhorar o desempenho da mesma.

A Gestão de Segurança, deve ser cada vez mais tida em conta, no sentido de garantir a integridade e impedir o acesso à rede ou através da mesma.

2.2.1. MODELO OSI

O modelo de referência *Open System Interconnection* (OSI) proposto pela ISO, um organismo internacional de normalização, constitui uma referência na adopção de normas relativas a redes de comunicações. No entanto, a mais-valia obtida com a possibilidade de constituir sistemas globalmente normalizados colide com a complexidade de implementação de sistemas baseados num modelo complexo como o OSI.

A utilização do modelo OSI assume maior importância nas redes de telecomunicações e constitui uma boa base de trabalho para as tecnologias emergentes.

A arquitectura proposta divide as redes de computadores em sete camadas, com funcionalidades específicas, de forma a se obter camadas de abstracção, que interagem com as camadas superiores e inferiores, Figura 2.1.

Figura 2.1 - Modelo OSI

1 - Camada Física

A camada Física trata, tal como o nome indica, das características técnicas dos dispositivos eléctricos (físicos), como placas de rede, cablagem e tipo de modulação. Define o controlo do acesso ao meio, controlo de qualidade e velocidade de transmissão e transforma os bits na medida eléctrica/óptica indicada.

2 - Camada de Enlace ou Ligação de Dados

Nesta camada são detectados e corrigidos os erros que possam acontecer na camada anterior, além de estabelecer o protocolo de comunicação entre sistemas directamente ligados e realizar o controlo de fluxo.

3 - Camada de Rede

A terceira camada é responsável pelo encaminhamento das ligações lógicas, ou seja pelo endereçamento dos pacotes, convertendo endereços lógicos (endereços IP) em endereços físicos, determina a rota que os pacotes devem seguir para atingir o destino, baseando-se em factores como condições de tráfego da rede e prioridades.

4 - Camada de Transporte

A camada de Transporte utiliza os dados recebidos pela camada superior, dividindo-os em pacotes que possam ser transmitidos para a camada de rede. Neste processo é realizado, controle de fluxo, ordenação dos pacotes e a correcção de erros, normalmente através do envio de sinais de confirmação (ACK) para o emissor. A camada 4 determina a classe de serviço necessária como orientada a conexão e com controlo de erro e serviço de confirmação, sem conexões e sem confiabilidade.

5 - Camada de Sessão

A camada de Sessão é fundamental para que duas aplicações em computadores diferentes estabeleçam uma sessão de comunicação. A sessão é definida pela forma como será feita a transmissão de dados e coloca marcações nos dados que estão a ser transmitidos.

6 - Camada de Apresentação

A camada de Apresentação tem como função a conversão da representação de dados num formato comum a ser utilizado na transmissão, entendido pelo protocolo usado.

7 - Camada de Aplicação

A camada de Aplicação faz a interface entre o protocolo de comunicação e o aplicativo que envia ou recebe os dados através da rede.

O Modelo OSI surgiu em 1977. Nessa altura o uso das redes de computadores passou a ser uma realidade crescente, assim como o aparecimento de novas tecnologias de rede. No entanto, todas elas proprietárias o que dificultava a sua interligação, sendo que em muitos casos era mesmo impossível fazê-lo.

Com a implementação do modelo proposto pela ISO, criou-se um modelo que permitiu aos fabricantes a criação de redes compatíveis com outras redes, padronizando componentes, permitindo o desenvolvimento paralelo, o que favoreceu em grande medida o crescimento posterior do uso desta tecnologia de comunicação.

O Modelo OSI tem associado um modelo de gestão baseado no protocolo *Commom Management Information Protocol* (CMIP)

Este protocolo utiliza os serviços de gestão da camada de aplicação, denominados de *Common Management Information Service* (CMISE), que suportam o acesso aos Objectos Remotos Geridos e a execução de operações sobre esses objectos. Estes serviços permitem a comunicação entre aplicações gestoras de rede e agentes de gestão. Este Modelo de Gestão surgiu para efectuar a gestão de redes que operem sobre o Modelo ISO, resultando em várias recomendações. Na sua versão inicial, este protocolo do nível de aplicação é suportado sobre a pilha de protocolos OSI. Porém, existe uma outra versão, denominada de CMIP *Over* TCPI/IP, isto é, CMOT, em que o protocolo é suportado sobre a pilha de protocolos Internet. Nesta versão, o protocolo é suportado em TCP/IP, sendo normalmente utilizada a Classe de Transporte 0, num serviço orientado-à-ligação, ou a Classe de Transporte 4, num serviço não orientado-à-ligação.

Dada a complexidade e requisitos necessários para a utilização de agentes e sistemas de gestão, o CMIP não obteve grande sucesso. Actualmente, praticamente todos os dispositivos suportam SNMP, mas não CMIP. Para o CMIP ficou reservado apenas dispositivos de telecomunicações.

2.2.2. MODELO TCP/IP

As origens do Modelo *Transmission Control Protocol/Internet Protocol* (TCP/IP) remontam aos finais da década de 60, mais concretamente 1969, quando o Departamento de Defesa (DoD) dos Estados Unidos desenvolveu, através da *Advanced Research Projects Agency* (ARPA), uma das primeiras redes de comutação de pacotes, a *ARPAnet*, que foi o embrião da Internet. No início da década de 70 foram criados organismos de normalização, nomeadamente o *Internet Architecture Board* (IAB), tendo a seu cargo a aprovação de documentos, *Request For*

Comments (RFCs), que passaram a definir a pilha protocolar TCP/IP. Até meados da década de 80 a utilização do TCP/IP e da Internet, era praticamente limitada a organismos militares e de educação. A partir dos anos 90 e paralelamente aos esforços para desenvolver normas internacionais como o modelo OSI, deu-se também o crescimento desenfreado da Internet em ambiente comercial, o que aumentou significativamente a importância das soluções de gestão da própria rede.

Tal como o modelo OSI, o modelo TCP/IP também funciona por camadas. Que se decompõe em vários módulos que efectuam cada um deles uma tarefa precisa.

Relativamente ao modelo OSI, o modelo TCP/IP simplifica-o, reduzindo o número de camadas de sete para quatro, Figura 2.2.

Figura 2.2 - Modelo TCP/IP

1 - Camada Acesso á Rede

Esta camada lida com os aspectos de ligação ao meio físico, sejam detalhes físicos ou lógicos. Corresponde à camada Física e de Ligação de Dados do Modelo OSI.

2 – Camada Internet/Rede

A segunda camada do Modelo TCP/IP é responsável pela circulação de *datagramas* na rede, encaminhando-os com base nos endereços IP destino. A fragmentação e reassemblagem dos pacotes também podem ser realizadas nesta camada, de forma a se ajustarem ao tamanho máximo suportado pela rede em causa. A importância desta camada é vital já que é responsável por todo o encaminhamento.

3 – Camada Transporte

A camada de Transporte assegura o correcto encaminhamento dos dados, entre a origem e o destino. São também da responsabilidade desta camada os aspectos relacionados com a qualidade de serviço, confiabilidade, controlo de fluxo e correcção de erros.

4 – Camada de Aplicação

Nesta camada são definidos os protocolos de aplicação e como os programas funcionam em interface com serviços de camada de transporte para utilizar a rede. Hoje em dia existem um número infindável de protocolos neste nível e para as mais diversificadas funções (*mail*, transferência de ficheiros, acesso remoto, vídeo chamada, voz sobre IP, etc.).

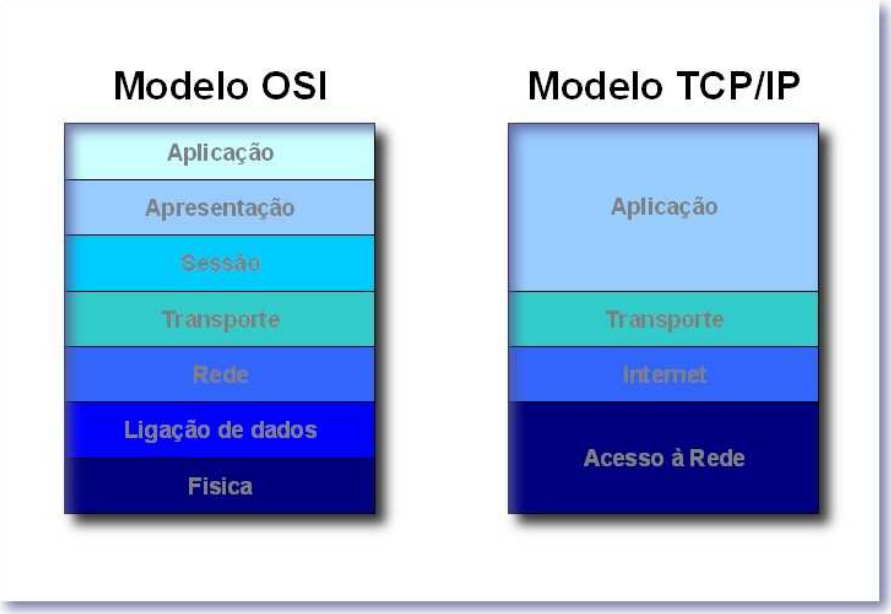

Figura 2.3 - Modelo OSI e Modelo TCP/IP

Apesar de similar ao modelo OSI, este modelo rompeu com muitos aspectos definidos pelo modelo OSI. Enquanto o modelo OSI foi pensado teoricamente, definindo todos os aspectos que poderiam ocorrer, o modelo TCP/IP tornou-se muito mais prático, e o seu desenvolvimento foi realizado de forma a resolver problemas reais, Figura 2.3.

2.2.3. MODELO TMN

O Modelo *Telecommunications Management Network* (TMN) é um conjunto de padrões internacionais especificados pelo *International Telecommunications Union – Telecommunication Standardisation Sector* (ITU-T), baseado no Modelo OSI para gestão de rede de telecomunicações.

O modelo TMN é definido por camadas, criando assim uma abstracção que permite que este modelo seja utilizado em redes e sistemas heterogéneos, Figura 2.4.

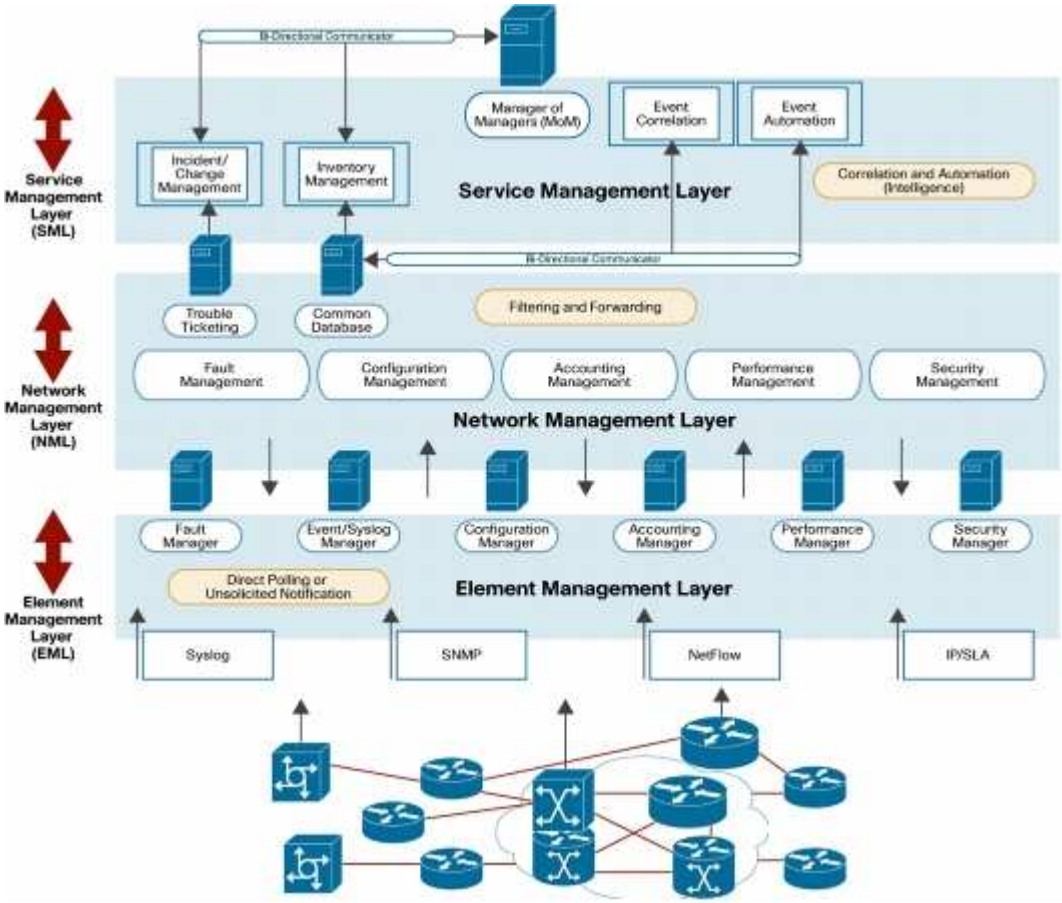

Figura 2.4 - Modelo TMN

Camadas lógicas do modelo TMN:

- Camada Gestão Negócios (BML - *Business Management Layer*) – desempenha funções ao nível do negócio, coordena o planeamento de alto nível, as estratégias, as decisões executivas;

- Camada Gestão de Serviços (SML – *Service Management Layer*) – Utiliza informação disponibilizada pela camada de gestão de rede (NML) para gerir contratos de serviço de clientes existentes e em potencial, desde o aprovisionamento e a qualidade de serviço, até à gestão de falhas. A camada SML é também responsável pela interacção com os provedores de serviços e com outros domínios administrativos, mantendo dados estatísticos para garantir a qualidade do serviço prestado;

- Camada Gestão Rede (NML – *Network Managemet Layer*) – Tem a visibilidade de toda a rede baseada em informações de Elementos de Rede (NE – *Network Element*)

disponibilizadas pelos sistemas operativos da camada de gestão de elemento de rede. A camada NML coordena todas as actividades de rede e suporta as requisições da camada SML;

- Camada Gestão Elementos de Rede (EML – *Element Management Layer*) – Gere cada elemento de rede. A camada EML possui vários monitores, cada um dos quais é responsável pelas informações passíveis de ser geridas dos *Network Elements* (NEs) específicos. De uma forma geral, um gerente de um NE é responsável por um subconjunto dos elementos de rede, gerindo os seus dados, actividades, registos, etc.;

- Elemento de Rede (NE – *Network Element*) representa o agente TMN, que apresenta as informações passíveis de ser geridas de cada um dos nós individualmente. O agente faz a interface entre a informação proprietária e a infra-estrutura TMN.

O modelo TMN define pontos de ligação entre elementos, que realizam os processos de comunicação, entre elementos do sistema de gestão, por exemplo, computadores geridos e unidade de gestão. Através de uma plataforma *standard* é possível que equipamentos de fabricantes diferentes comuniquem dentro da mesma rede, e sejam geridos por uma unidade central de gestão única.
Este modelo de gestão pode ser utilizado em redes de dados ISDN, B-ISDN, ATM ou GSM, sendo já utilizado em operadores de telecomunicações como a AT&T, Sprint, France Telecom, Telefónica entre outras.

2.2.4. MODELO DE GESTÃO SNMP

O modelo de Gestão *Simple Network Managment Protocol* (SNMP) é nos dias de hoje o protocolo padrão para a gestão de redes e intimamente ligado ao Modelo TCP/IP [1].
O protocolo SNMP [2] surgiu em 1988, através da publicação do RFC1052 [3] pela Internet *Architecture Board* (IAB). Este documento foi o ponto de partida para a especificação de um modelo de gestão de redes. Com o título "*IAB Recommendations for the Development of Internet Network Management Standards*", explicava em que consistia a gestão de redes de dados. Alguns dos objectivos eram:

- Ser o mais abrangente possível;

- Suportar o maior número de equipamento;

- Suportar o maior número de protocolos;

- Ser expansível.

Foi evoluindo ao longo dos anos, sendo acrescentadas novas funcionalidades e suporte a um maior número de dispositivos e protocolos.

Actualmente na versão 3, fornece a possibilidade de monitorizar dispositivos ligados em rede, através do envio de pedidos sobre o seu estado. Permite ainda proceder a configurações desses mesmos dispositivos remotamente, o que poderá ser uma mais-valia no caso de se pretender que o sistema de monitorização seja capaz de responder de uma forma automática a incidentes.

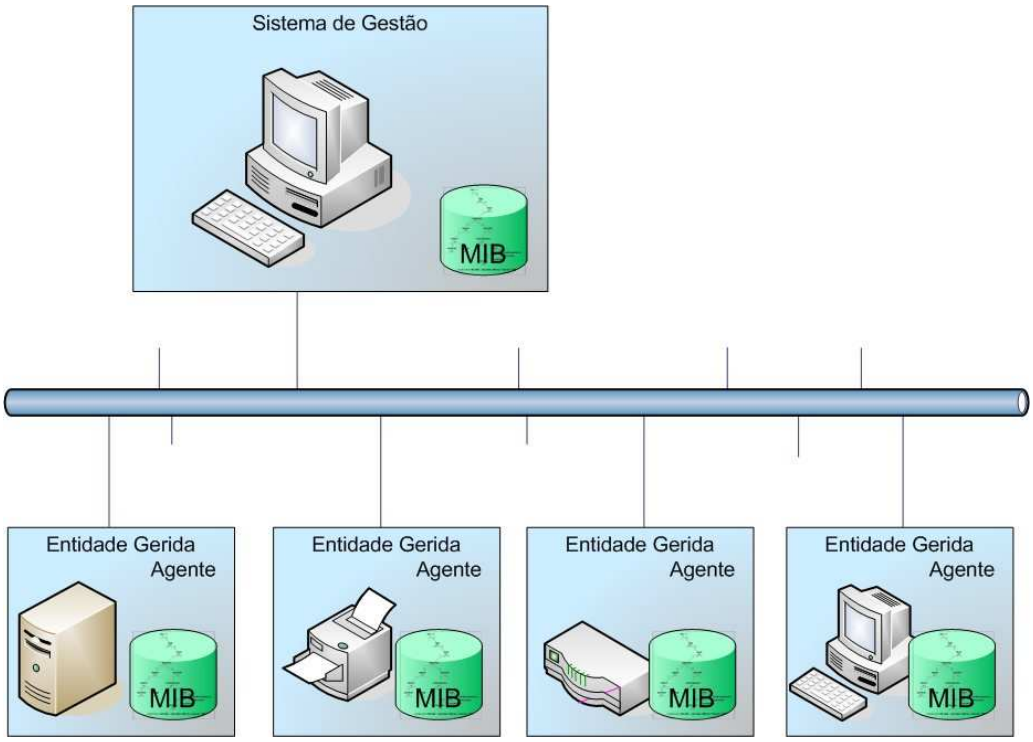

Figura 2.5 - Sistema de Gestão SNMP

2.2.5. ARQUITECTURA DO MODELO DE GESTÃO TCP/IP

O modelo de gestão que se aplica às redes TCP/IP é constituído por quatro elementos base, Figura 2.5: Sistema de Gestão (Estação de Gestão); Entidade Gerida (Agente); Protocolo de Gestão (SNMP); e a Base de Dados com Informação de Gestão (MIB).

O Sistema de Gestão (Estação de Gestão) – central ou distribuído – é responsável pelas aplicações que monitorizam e controlam as Entidades Geridas (Agentes). Basicamente, a gestão é feita através da disponibilização das *Management Information Bases* (MIBs) pelo Agente à Estação de Gestão, sendo a comunicação estabelecida através do protocolo SNMP, que suporta primitivas básicas para a troca de informação entre duas entidades. Esta informação, acedida através do SNMP, é a base do funcionamento da maioria das aplicações de gestão de redes actuais.

A MIB é um repositório conceptual de dados residente nas Entidades Geridas (Agentes), que é acedido pelos Gestores através do protocolo de gestão SNMP.

Os padrões de gestão OSI e Internet definiram MIBs que representam os objectos necessários para a gestão dos seus recursos. Por outro lado, as regras de construção das estruturas da MIB são descritas através da *Structure of Management Information* (SMI) [4]. Esta estrutura é um conjunto de documentos que definem: forma de identificação e grupos de informação; sintaxes permitidas e tipos de dados permitidos.

O princípio assenta em utilizar um esquema comum para representar os objectos, ou seja, os objectos são definidos de uma forma padronizada, o que permite a sua codificação para a transferência na rede.

A semântica definida pela SMI apresenta a informação segundo uma árvore, Figura 2.6.

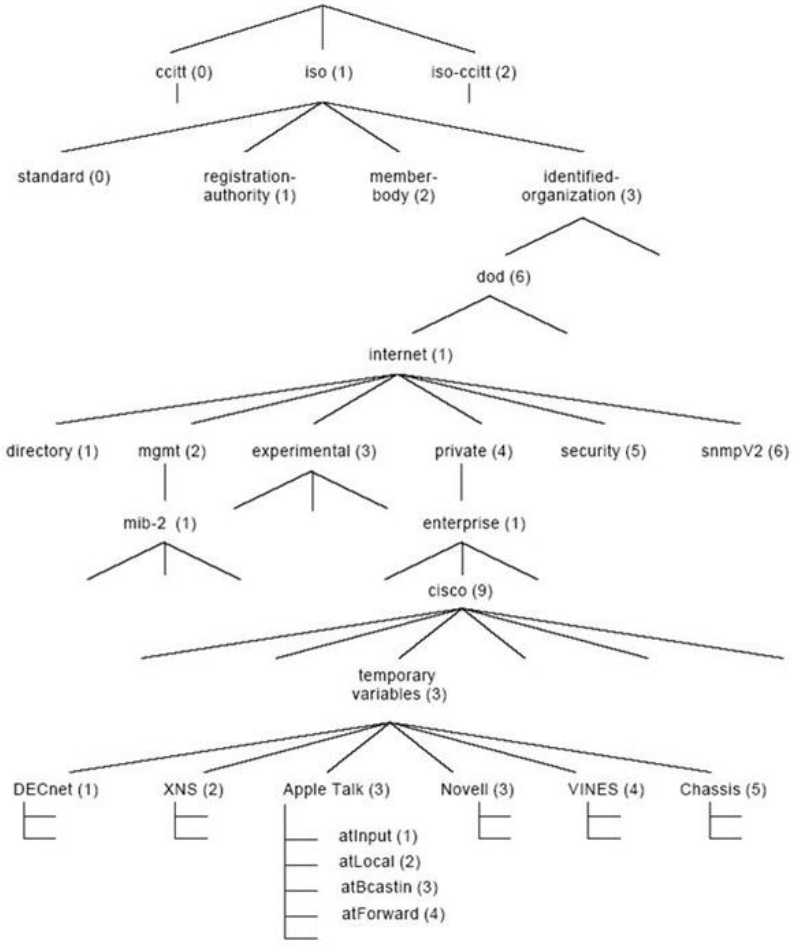

Figura 2.6 - Excerto de uma MIB

Os objectos ou variáveis das MIBs são definidos formalmente na notação *Abstract Syntax Notation.1* (ASN.1) [5] e são identificados univocamente através de uma sequência de números inteiros separados por pontos, indicando o caminho a percorrer na árvore da MIB. Este número identificativo é utilizado nas mensagens SNMP. Por exemplo, para identificar os atributos específicos da Cisco o *Object Identifier* (OID) é **1.3.6.1.4.1.9**.

A linguagem ASN.1 é utilizada também para definir os *Protocol Data Unit* (PDUs), utilizados pelo SNMP na comunicação entre a Estação de Gestão e a Entidade Gerida.
O protocolo SNMP suporta primitivas básicas para a troca de informação entre duas entidades, Figura 2.7. Na primeira (1) versão do SNMP, apenas quatro primitivas estavam implementadas:

- GET, usado pela Entidade Gestora para pedir um parâmetro à Entidade Gerida (Agente), ou seja, obter uma determinada informação;
- GETNEXT, utilizado para, interactivamente, obter informações sequências da MIB da Entidade Gerida;
- SET, permite alterar um parâmetro de configuração na Entidade Gerida;
- TRAP, primitiva desencadeada assincronamente pela Entidade Gerida, para notificar a Entidade Gestora de que algum valor na sua MIB (Agente) foi alterado.

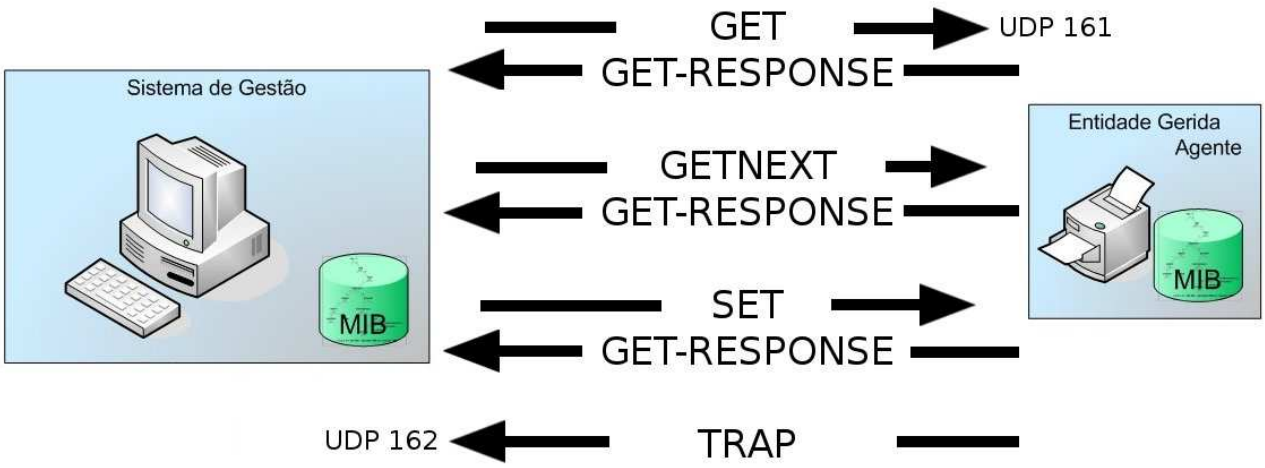

Figura 2.7 - Funcionamento Mensagens SNMP

Na segunda (2) versão deste protocolo, foram introduzidas novas funcionalidades e novas primitivas. Nomeadamente:

- A primitiva GET-BULK, com o objectivo de ser possível com um só pedido obter uma quantidade maior de informação (sequencial);
- A primitiva INFORM, utilizada para a transferência de informação entre Entidades Gestoras.

- Por último, a primitiva REPORT definida na segunda (2) versão do SNMP, mas nunca implementada, passou a *standard* na terceira (3) versão, e tem por finalidade, permitir a comunicação entre Entidades Gestoras SNMP.

Além das novas primitivas introduzidas, com a segunda (2) versão do protocolo SNMP, foram também introduzidos novos aspectos relacionados com questões de segurança. No entanto, só com a publicação da terceira versão (3), o SNMP foi finalmente contemplado com verdadeiros mecanismos de segurança. O SNMPv3 surge como o reunir e culminar de um esforço desenvolvido em vários sentidos, tendo por base de trabalho as duas iniciativas relativas à implementação de segurança no SNMP, formalmente conhecidas por SNMPV2* e SNMPV2u [6] [7] [8] [9].

A terceira (3) versão passou a dispor de criptografia simétrica, quer para autenticação, quer para o envio de dados.

A implementação destes mecanismos de segurança aproveita os formatos das mensagens das anteriores versões, Figura 2.8.

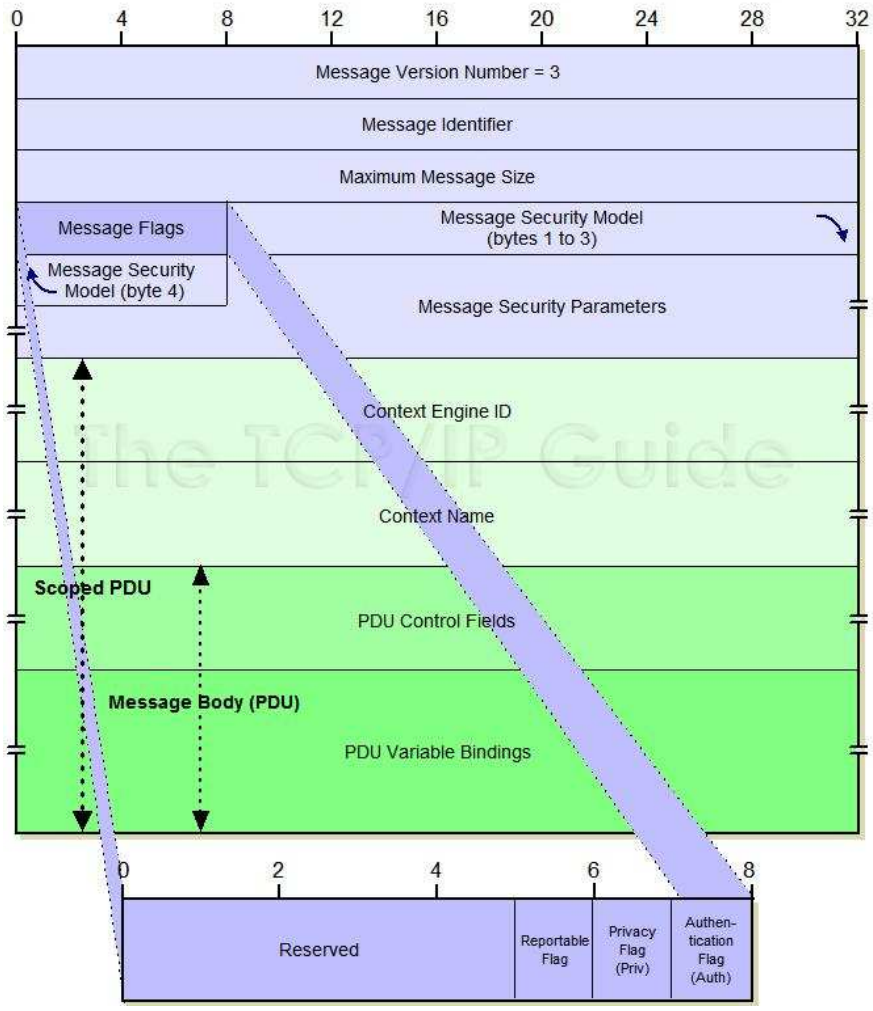

Figura 2.8 - Arquitectura protocolar do SNMPv3

A arquitectura de Gestão SNMPv3 [10] é constituída por um conjunto de entidades SNMP distribuídas, que cooperam entre si. Cada entidade implementa uma parte da arquitectura SNMP, podendo funcionar como Agente, Gestor ou ambos em simultâneo.

Esta arquitectura foi desenvolvida segundo módulos, tendo em vista o posterior aperfeiçoamento de cada módulo de forma independente. Cada entidade é constituída por um conjunto de módulos que interagem entre si para providenciar serviços. Sendo as interacções modeladas através dum conjunto de primitivas abstractas e parâmetros.

Uma entidade SNMP [11] é composta por um motor SNMP, identificado pelo identificador *snmpEngineID* e as aplicações SNMP, Figura 2.9.

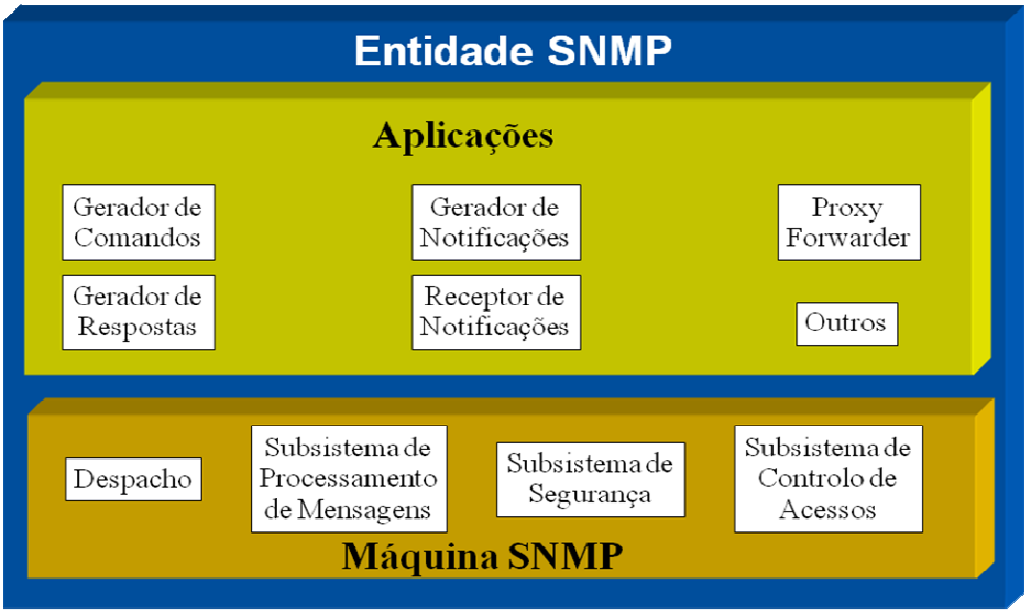

Figura 2.9 - Entidade SNMP

O papel desempenhado por uma entidade SNMP é definido pelos módulos que essa entidade implementa, assim um Agente e um Gestor possuem módulos diferentes. Esta modularidade permite também a definição de versões diferentes de cada módulo, implementando novas funcionalidades sem a necessidade de se efectuar uma revisão de toda a norma.

O SNMP assenta no modelo cliente-servidor sendo a Entidade Gestora responsável por recolher a informação de gestão proveniente das Entidades Geridas, as quais podem ser implementadas nos mais diversos equipamentos, fornecendo informação de gestão normalizada, ou proprietária para ser utilizada pelas aplicações de gestão adequadas.

Numa rede não é necessário que todos os equipamentos implementem um agente SNMP, desde que exista um Agente Procurador (*Proxy*) capaz de fornecer informações sobre os primeiros, ou seja, capazes de dialogar com os primeiros.

2.2.6. REMOTE NETWORK MONITORING (RMON) MIB

A RMON MIB surgiu com o objectivo de proporcionar uma gestão mais flexível, uma vez que oferecia uma arquitectura de gestão distribuída. A implementação da RMON MIB propunha alcançar os seguintes objectivos: análise de tráfego, análise de tendências e gestão pró activa [12].

Além destes objectivos, pretendia-se dotar a RMON MIB da capacidade de operar off-line. Uma vez que os agentes das Entidades Geridas poderão não estar sempre em contacto com a Estação de Gestão, estes devem ser suficientes de realizar diagnósticos de forma contínua e guardas os resultados obtidos, até ser possível notificar a Estação de Gestão e enviar os dados acumulados.

Enquanto que um Agente SNMP monitoriza o activo em que está instalado, através da arquitectura RMON MIB é possível analisar um segmento de rede, a partir de um ponto central (RMON *Probe*), de forma a detectar problemas como congestionamento de tráfego, pacotes perdidos ou colisões. Além da monitorização em tempo real é possível definir valores padrão que se não se verificarem, despoletarão alarmes, para que se possam tomar as medidas correctivas necessárias. Estes Agentes RMON, Figura 2.10, analisam o segmento de rede onde estão inseridos, recolhendo e processando informações, que são depois enviadas para o Sistema de Gestão da rede. Desta forma obtém-se uma redução de tráfego e processamento, quando comparado com o funcionamento tradicional.

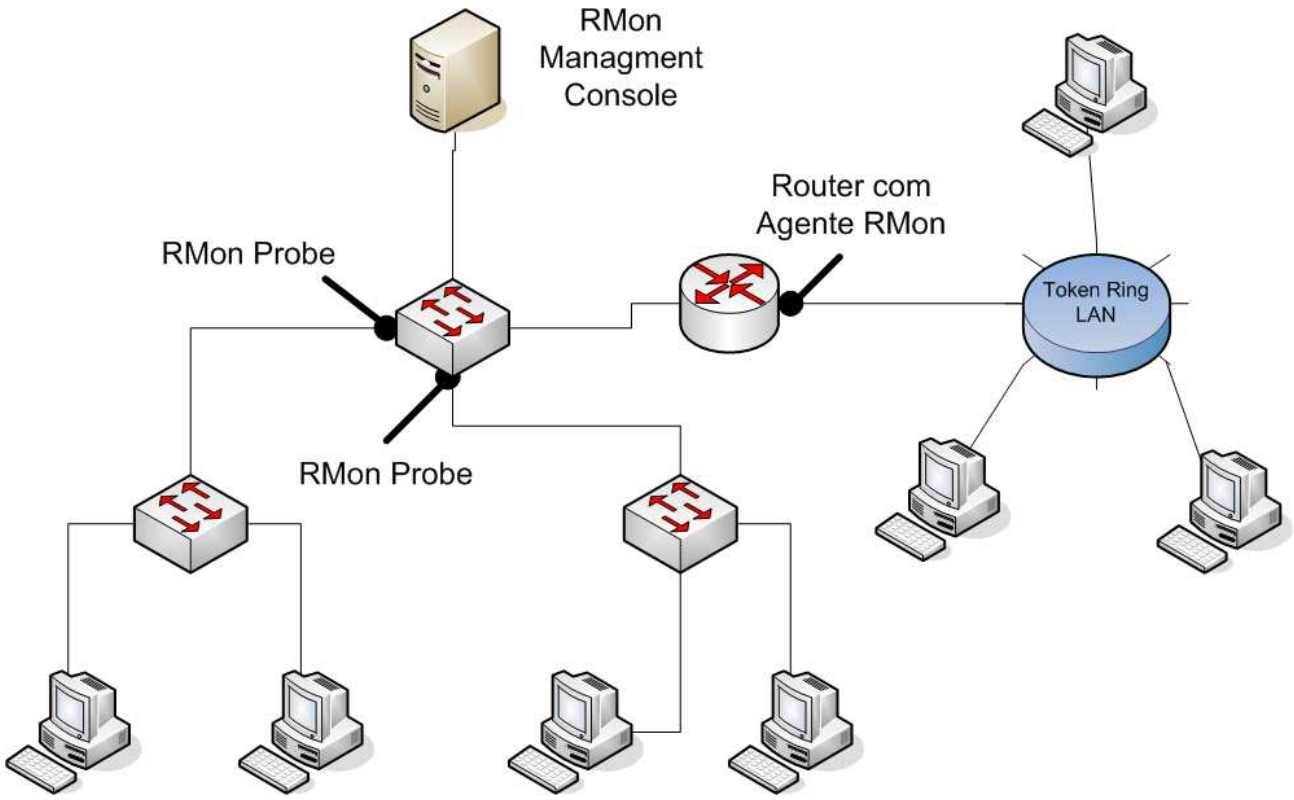

Figura 2.10 - RMON

A primeira versão, comummente denominada RMON1, está vocacionada apenas para as duas camadas mais baixas do Modelo OSI (Ligação de Dados e Física) e para redes *Token Ring*. Foi mais tarde actualizada, passando a suportar também as camadas 3 a 7 do Modelo OSI (Rede e Aplicação respectivamente), Figura 2.11.

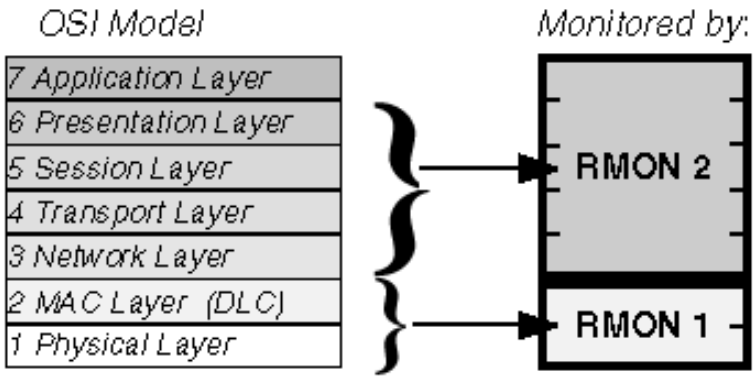

Figura 2.11 - Modelo OSI e Implementação RMON

Tal como no SNMP, a RMON possui uma base de dados de informação monitorizável (RMON MIB), partilhada entre Entidades Gestoras e Agentes (ou "*Probes*" tal como são designados na RMON)

A primeira versão da RMON, Figura 2.12, apenas possuía dez (10) grupos de objectos:

1. *Statistics* – Estatísticas em tempo real, tais como utilização, colisões, erros, etc.;
2. *History* – Histórico de estatísticas seleccionadas;
3. *Alarm* – Definição de *Traps* SNMP enviados quando as estatísticas ultrapassam valores pré-definidos;
4. *Hosts* – Estatísticas por *Host*: *bytes* enviados/recebidos, *frames* enviadas/recebidas;
5. *Top Hosts* – Registo do top de estatísticas de *host*;
6. *Matrix* – Matriz de tráfego (enviado/recebido) entre sistemas;
7. *Filter* – Definição de tipo de tráfego, tal como endereço MAC ou porto TCP;
8. *Capture* – Recolha e encaminhamento de pacotes definidos por um Filtro;
9. *Event* – Envio de *Traps* para o grupo *Alarm;*
10. *Token Ring* – Extensão com dados específicos de redes *Token Ring.*

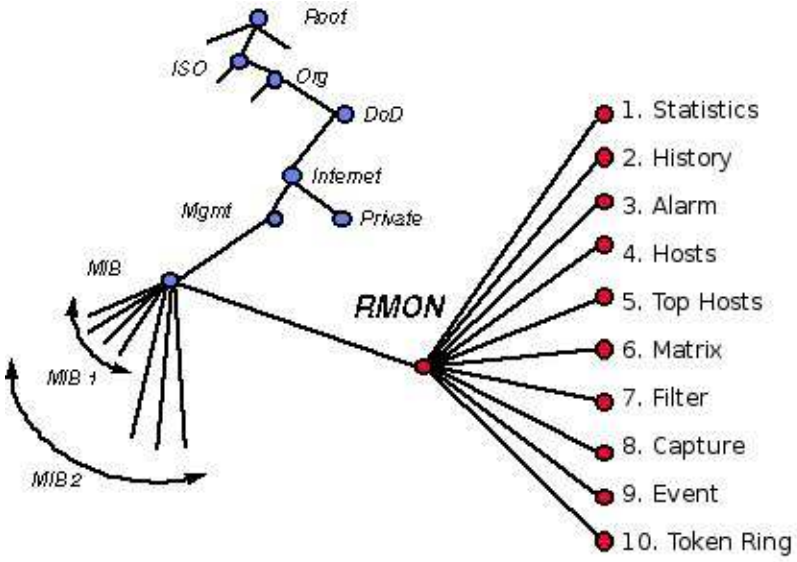

Figura 2.12 - MIB RMON v1

Existem agentes RMON que implementam apenas os objectos Estatística, Histórico, Alarmes e Eventos. Equipamentos que apenas suportam estes objectos da RMON MIB, normalmente designam-nos como "*mini RMON*" ou "*Four Pack RMON*", sendo estes objectos suficientes para analisar colisões. Alguns activos de rede que apenas implementam a versão reduzida da RMON são *switchs* da D-*Link, Cisco* ou *3Com*.

Com o aparecimento da RMON2, Figura 2.13, também a MIB respectiva foi actualizada, sendo acrescentados mais dez (10) novos grupos:

1. *Protocol Directory* – Lista de protocolos monitorizáveis;
2. *Protocol Distribution* – Estatísticas de tráfego por protocolo;
3. *Adress Map* – Tabela de referências: endereço MAC e endereço IP;
4. *Network-Layer Host* – Estatísticas da camada 3 (Rede), por *Host*;
5. *Network-Layer Matrix* – Estatísticas da camada 3 (Rede), por par de *Hosts*;
6. *Aplication-Layer Host* – Estatísticas da camada 7 (aplicação), por *Host*;
7. *Aplication-Layer Matrix* – Estatísticas da camada 7 (aplicação), por par de *Hosts*;
8. *User History* – Valores periódicos para variáveis definidas;

9. *Probe Configuration* – Configuração remota dos "*Probes*";

10. RMON *Conformance* – Necessário para conformidade.

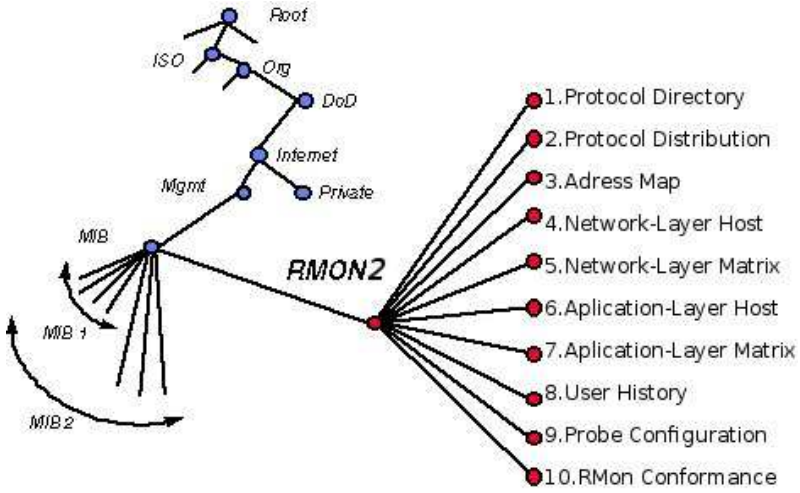

Figura 2.13 - MIB RMON v2

Um *Probe*, além da capacidade de analisar o segmento de rede onde está inserido, disponibiliza a capacidade de gestão dele próprio através da implementação da MIBII [13].
A arquitectura RMON é definida no RFC1757 [14] para gestão proactiva de redes. Funciona sobre a pilha TCP/IP, integrado no SNMP. A RMON2 é capaz de realizar um mapeamento de todos os grupos do RMON, na maioria dos protocolos de rede: IP, IPX, DECnet, AppleTalk etc.

2.3. MODELOS DE GESTÃO DE SISTEMAS

Tal como as redes informáticas necessitam de ferramentas de monitorização e gestão, também os sistemas computacionais complexos, necessitam de ser acompanhados, monitorizados e actualizados.
As funções associadas à gestão de sistemas passam pela actualização do software, monitorização e controlo remoto dos sistemas, gestão das licenças, inventário de hardware e software, ou seja, todo um vasto conjunto de potencialidades que deverá ser compatibilizado com as ferramentas e mecanismos tradicionais de gestão de redes

2.3.1. DMI – DESKTOP MANAGEMENT INTERFACE

O DMI, Figura 2.14, é uma base normalizada para a gestão e controlo de computadores, sejam postos de trabalho, portáteis ou servidores, abstraindo os dispositivos geridos do software que os gere. Foi o primeiro passo (em 1994) dado pela *Distributed Management Task Force* (DMTF), na

gestão de sistemas, beneficiando o ambiente de computação de rede onde inúmeros computadores são geridos.
O DMI pode coexistir com o SNMP ou outros protocolos de gestão, sendo o DMI responsável por responder a pedidos realizados (SNMP *Query*) pela Entidade Gestora SNMP.
O DMI é independente do hardware ou sistema operativo, sendo acessível a adopção por parte de fabricantes

DMI é composto pelos seguintes componentes:

- *Management Information Format* (MIF): trata-se de um ficheiro de texto que contem toda a informação do hardware e software utilizado no computador. O ficheiro MIF contém os atributos que descrevem cada um dos componentes (Número identificador, Nome Produto, Versão, Número de Série, Data e Hora da ultima instalação). As MIFs podem ser expansíveis pelos fabricantes, de forma a se adaptar aos vários produtos, ou categorias de produtos, como por exemplo equipamento de Fax;

- *Service Layer*: Este é uma aplicação residente em memória que faz a interligação entre *Management Interface* (MI) e a *Component Interface* (CI), permitindo o acesso à informação guardada na MIF. Esta aplicação é disponibilizada como um serviço do sistema operativo e acessível por todos os programas;

- *Component interface* (CI): Esta aplicação é uma interface que envia informações de estado para o ficheiro MIF respectivo através da *Service Layer*. Esta API (*Application Program Interface*) disponibiliza comandos *Get* e *Set*, de forma a interagir com a MIF à medida das necessidades;

- *Management interface* (MI): A MI também se trata de uma aplicação que permite a comunicação com o Sistema de Gestão. Facilita que o administrador/gestor dos sistemas envie comandos *Set* e *Get*, bem como, listar todos os dispositivos geridos através de DMI.

Apesar da capacidade de monitorizar tanto o hardware como software, esta tecnologia acabou em desuso, terminando em Março de 2005, dando lugar a tecnologias mais avançadas como o CIM.

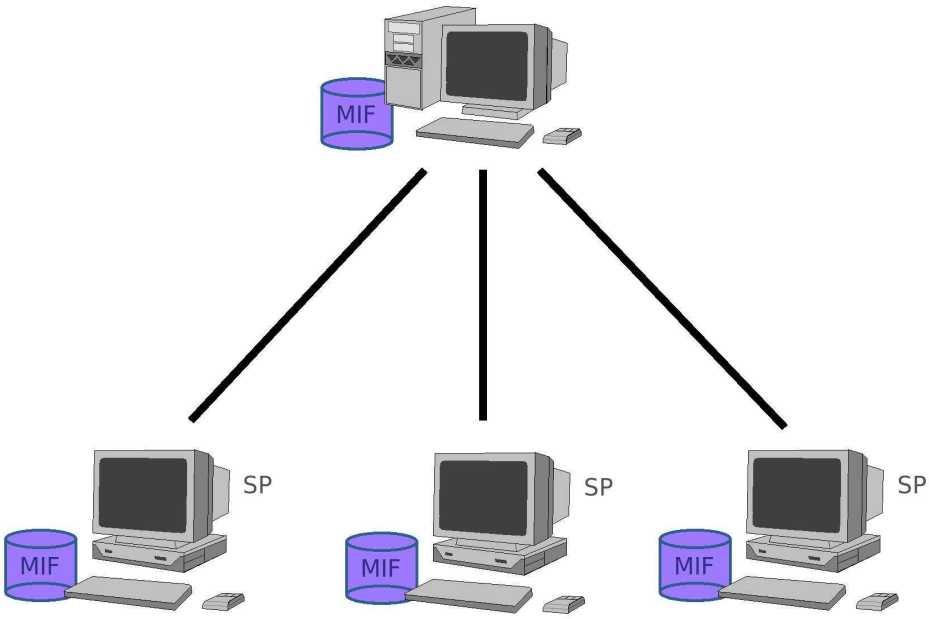

Figura 2.14 - Desktop Management Interface

2.3.2. CIM – COMMON INFORMATION MODEL

O modelo CIM é um *standard* aberto que define como os elementos são geridos num ambiente informático, descrevendo a sua representação e relações entre eles, criado de forma a permitir a gestão entre elementos, independentemente do fornecedor ou proprietário.

Os grandes fabricantes de hardware (Cisco, 3COM, Compaq, Dell, HP, Intel, IBM ou Novell) bem como a *Microsoft* aderiram à norma CIM, apoiando o seu desenvolvimento. Este modelo define a Infra-estrutura CIM e o CIM *Schema*, Figura 2.15.

A infra-estrutura (*CIM Specification*) define a arquitectura e os conceitos do modelo, incluindo a notação e o método de interligação com outros modelos, como o SNMP.

Esta arquitectura é baseada em UML (representada através de XML) e orientada aos objectos (*Object Oriented*), sendo os Elementos Geridos definidos por classes, havendo relações e herança entre classes.

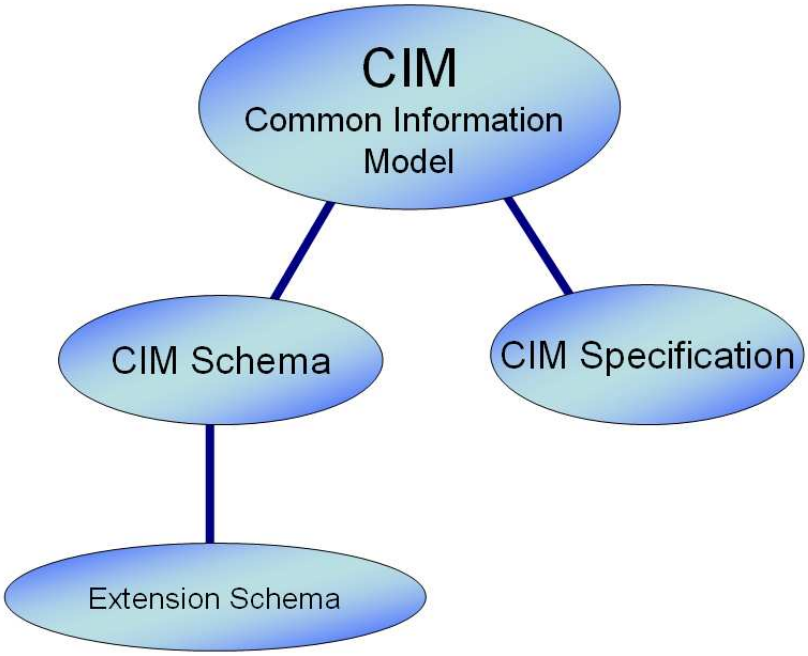

Figura 2.15 - Common Information Model

Schema CIM é conceptual e define os objectos que podem ser geridos. Actualmente a quase totalidade de elementos num ambiente TI, podem ser representados, desde computadores, sistemas operativos, redes, aplicações ou serviços. Mas uma vez que muitos Elementos Geridos possuem características próprias o *Schema* CIM é extensível de forma a suportar representações e comportamentos específicos.

A última versão da arquitectura CIM (versão 2.5) foi publicada em Maio 2009 e do *Schema* (versão 2.22) em Junho de 2009.

2.3.3. JMX – JAVA MANAGEMENT EXTENSIONS

A tecnologia JMX fornece ferramentas para desenvolver soluções de gestão e monitorização de dispositivos [15], de forma distribuída, modular e dinâmica, com uma interface Web.

Em desenvolvimento pela Sun *Microsystems* há vários anos (desde 1996), era denominado por JMAPI, alterando o nome para JMX, em 1999, quando saiu a segunda versão das especificações.

O objectivo da JMX, é fornecer de uma forma simples a gestão de objectos, independentemente do modelo de gestão escolhido, seja TMN ou SNMP, por exemplo.

Os dispositivos monitorizados – equipamentos, aplicações, serviços – são representados ao nível da programação por objectos, identificados por *MBeans* (*Managed Bean*).

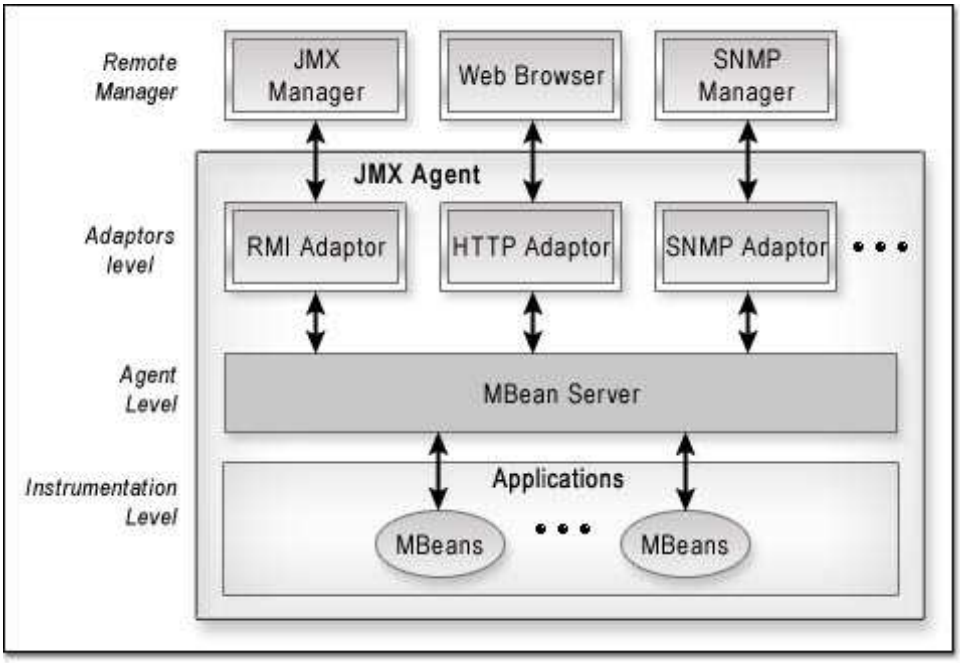

Figura 2.16 - Arquitectura JMX

A arquitectura do JMX, Figura 2.16, assenta em três especificações principais:

O **nível instrumental** (*Instrumentation Level*) defina a implementação dos recursos geridos, que podem ser aplicações, serviços ou dispositivos, tendo como uma única condição o facto de serem escritos em Java. A instrumentação é definida por *Managed Beans*. Esta camada define os recursos para que possam ser geridos pela Entidade Gestora e os *MBeans* são desenvolvidos de forma a ser genéricos, flexíveis e de fácil implementação. É também neste nível que são implementados os alertas.

A **camada agente** (*Agent Level*) especifica os Agentes de Gestão, controlando recursos e disponibilizando-os para outras aplicações. Este nível funciona como intermediário com a camada instrumental, fornecendo um agente normalizado para o sistema JMX.

O **nível de adaptadores** (*Adaptor level*), apesar de ainda não se encontrar completamente definido na arquitectura JMX, pretende representar os componentes que podem interagir com os *MBeans*.

2.3.4. WBEM - WEB BASED ENTERPRISE MANAGEMENT

O WBEM é um conjunto de tecnologias de gestão desenvolvidas para uniformizar a gestão e monitorização de sistemas distribuídos, criado inicialmente pela *Microsoft*, Compaq e Cisco, em 1998 tornou-se uma norma da DMTF. É baseado nos *standards* da Internet e no DMI (particularmente na evolução do DMI – o CMI) e com um funcionamento similar ao SNMP, Figura 2.17.

O WBEM é extensível, independente do sistema operativo, com ferramentas e aplicações reutilizáveis. Além da utilização por vendedores e utilizadores finais, o WBEM está a ser

desenvolvido e utilizado noutras áreas, tais como serviços Web, segurança ou sistemas de *Backup*.

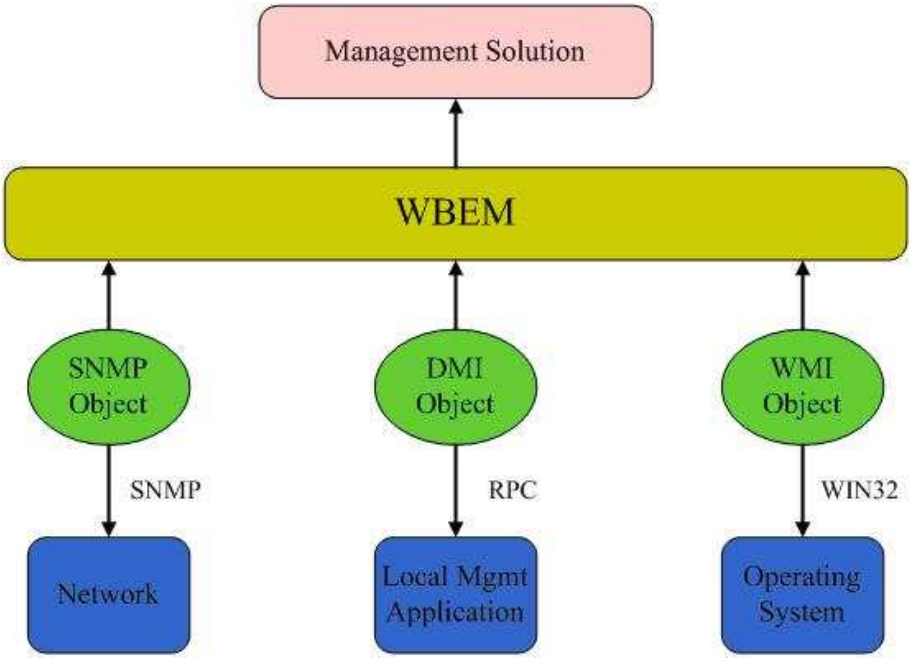

Figura 2.17 - WBEM

Actualmente já existem diversificadas implementações do WBEM, de destacar:

- *Apple* implementou o WBEM, na ferramenta *Apple Remote Desktop*;
- *Novell* adoptou o *OpenWBEM* (uma implementação livre do WBEM), que é distribuído no *SUSE Linux Enterprise Server*;
- *Sun Microsystems* criou o *WBEM-Services* para o sistema operativo *Solaris*;
- *Hewlett Packard* inclui serviços WBEM *Services* em todas as versões do sistema operativo HP-UX;
- *Red Hat* utiliza o *OpenPegasus* como parte do *Red Hat Enterprise Linux*.

3. PLATAFORMAS DE GESTÃO

3.1. INTRODUÇÃO

Com o crescimento da dimensão das Tecnologias de Informação (TIs), no seio das organizações, a necessidade de monitorização e ferramentas de apoio à gestão tem-se tornado primordial. Nas últimas décadas, o sistema informático deixou de ser um ou dois servidores e alguns computadores pessoais, passando a ser um sem fim de equipamentos, com inúmeras funcionalidades essenciais para o desenvolvimento da actividade principal das empresas. Servidores de rede, de ficheiros, de impressoras, activos de redes, fotocopiadoras, impressoras, faxes, sistemas de voz e vídeo sobre IP, vídeo vigilância, sistemas biométricos, etc., são hoje em dia comuns em qualquer empresa.

Actualmente existem disponíveis diversas plataformas de gestão de redes e plataformas de gestão de sistemas.

A gestão de redes é, desde há muito tempo, objecto de estudo e uma área que requer muita atenção por parte dos gestores de forma a manter as comunicações funcionais, assim como tirar o maior partido possível da infra-estrutura instalada. Com a interligação actual, dos mais variados equipamentos às rede IP, uma simples plataforma de gestão de rede deixa de ser capaz de assimilar as particularidades dos equipamentos que operam sobre a rede.

Uma plataforma de gestão de sistemas, visa dotar o gestor ou administrador, de informação sobre o estado global do sistema que administra, fornecendo informação em tempo real, informação estatística, etc. Além da recolha de informações deve também permitir automatizar as tarefas de gestão, centralizá-las, e fazer face ao dinamismo existente nos SI, sem ser necessário recorrer às interfaces individuais de cada dispositivo ligado à rede.

Neste capítulo, iremos analisar quais as características principais de uma plataforma de gestão, efectuar um estudo sobre as principais plataformas de gestão disponíveis no mercado com o objectivo de identificar as suas qualidades e deficiências. Sendo também efectuada uma análise comparativa das soluções estudadas. Faz-se, ainda um estudo sobre modelos de gestão de sistemas.

3.2. REQUISITOS PLATAFORMA DE GESTÃO

Para analisar uma plataforma de gestão é necessário definir as características principais que a caracterizam. A análise deve ter em conta diversos aspectos, quer a nível das funcionalidades implementadas, quer a nível do seu modo de funcionamento e interacção com o utilizador, assim como com outras plataformas e dispositivos.

As características a ter em conta devem ser adequadas às necessidades actuais de gestão de uma infra-estrutura informática. Pelo que, estabeleceu-se um conjunto de características que irá ser considerado na análise e que são a base de trabalho para o estudo a realizar.

Ao nível da plataforma, deve ser analisado o sistema operativo suportado, a interface gráfica disponibilizada e quais as funcionalidades extra suportadas, tais como: estatísticas fornecidas, gráficos fornecidos, integração com outras ferramentas e não menos importante o preço da aplicação.

Relativamente às funcionalidades incorporadas, devem ser analisados dois grandes grupos distintos: as funcionalidades relacionadas com a gestão de redes, tais como, *auto-discover* ou gestão de equipamento e as funcionalidades relacionadas com a gestão de sistemas, tais como gestão de políticas ou inventário de hardware e software.

Na tabela seguinte, Tabela 3.1, são enumeradas as várias características tidas em conta na análise efectuada a várias plataformas de gestão.

	Funcionalidades
Sistema	SO suportados instalação
	Interface com utilizador (GUI/Web)
	Integração com outras aplicações
	Estatísticas
	Gráficos de desempenho
	SNMP
	Envio de alertas
	Relatórios
Gestão Redes	*Auto-discover*
	Gestão de equipamentos
	Monitorização Remota (RMON)
	Processamento eventos
	Mapa de rede
Gestão Sistemas	*Auto-discover*
	Distribuição de software
	Gestão de políticas
	Inventário (Hardware e Software)
	Controlo remoto
	Controlo de licenças
	SO suportados gestão
Preço	

Tabela 3.1 - Análise Sistemas de Gestão

3.3. PLATAFORMAS DE GESTÃO GENERALISTAS

O crescimento da necessidade de acompanhar a evolução e o estado actual das redes, e dos seus equipamentos, teve como consequência o aparecimento no mercado de várias soluções. Assim, a oferta de aplicações de gestão tornou-se visivelmente crescente, sem que ninguém pretendesse perder a oportunidade. Desde marcas conceituadas, na área tecnológica, tais como IBM ou HP, até projectos sem fins lucrativos, como é o exemplo do *OpenNMS*, todas apresentaram as suas soluções, como sendo a mais completa e a melhor disponível no mercado.

3.3.1. HP OPENVIEW

Criado pela empresa *Hewlett Packard* (HP) consiste num conjunto de ferramentas para gestão de rede e de sistemas [16]. Capaz de gerir infra-estruturas de grande dimensão, este conjunto de aplicações inclui aplicativos desenvolvidos pela própria HP, bem como por terceiros.

Inicialmente, criada como *Network Node Manager* (NNM) consistia apenas numa interface gráfica, integradora de outros produtos. Actualmente, através de compras e fusões (2004 – *Novadigm Radia Suite*, 2005 - *Peregrine Systems*, 2006 - *Mercury Interactive Corp*), tornou-se numa aplicação integrada de gestão de redes e sistemas em ambientes de computação distribuída, nomeadamente nas áreas de Gestão de Redes, Sistemas, Aplicações e Qualidade de Serviço, Figura 3.1.

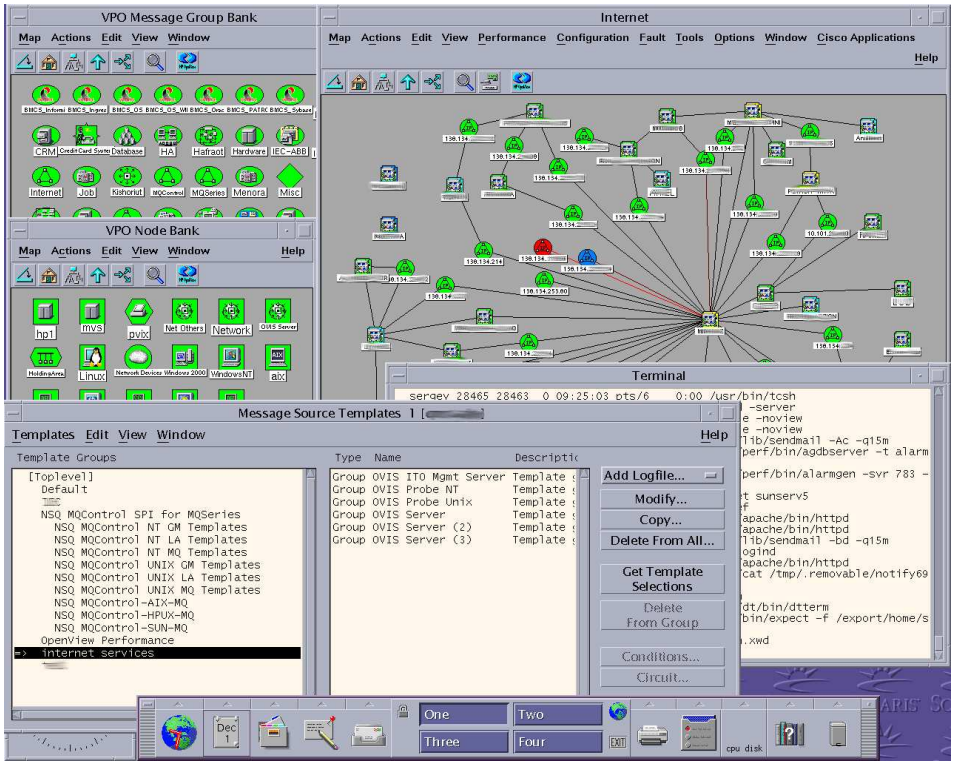

Figura 3.1 - HP OpenView

Uma outra característica importante é a disponibilização de uma interface Web para as suas aplicações de gestão, o que possibilita o acesso a partir de qualquer ponto da rede à aplicação de gestão.
A liderança no mercado da gestão, e um reconhecimento merecido ao longo de vários anos de domínio de mercado, fazem desta plataforma e da família *OpenView* uma das melhores soluções constituídas e com mais crédito na área da gestão.

Apesar de incluir variados módulos desenvolvidos pela HP, o OpenView pode ser integrado com produtos ou componentes desenvolvidos por terceiros através de uma *framework* bem definida.
Alguns das ferramentas integradas nesta aplicação são:

- *OpenView Network Node Manager*;
- *OpenView Reporter*;
- *OpenView Operations*;
- *OpenView Service Navigator*;
- *OpenView Service Desk*.

Integrações da plataforma HP *OpenView*:

- *Cisco*;
- *3Com*;
- *AirWave Wireless*;
- *Servidores SUN*;
- *IBM WebSphere*;
- *BMC Performance Manager*;
- *APC NetBotz*;
- *OpenNMS*;
- *Nagios*.

Considerada uma das quatro melhores aplicações de Gestão de sistemas, apresenta como pontos fortes o facto de possuir uma interface gráfica simples e eficaz e o infindável número de funcionalidades de base, como estatísticas, gráficos de desempenho, envio de alertas, *auto-discover* ou mapa de rede, assim como módulos opcionais e uma grande variedade de ferramentas que se podem integrar com o *HP OpenView*.

3.3.2. IBM TIVOLI NETVIEW

O *Tivoli Netview* [17] é apenas um dos componentes do produto *IBM Tivoli Enterprise Console*. Trata-se de um produto completo de gestão de eventos, que integra sistemas, rede, bases de dados e gestão de aplicações, de forma a assegurar a disponibilidade dos serviços TI de uma organização. Este objectivo é alcançado através de monitorização em tempo real [18], Figura 3.2.
O *NetView* é a aplicação responsável pela gestão de redes, e através do protocolo SNMP é capaz de descobrir, monitorizar e configurar redes TCP/IP, bem como gerir eventos e *traps* SNMP, assim como recolher informação sobre a performance da rede, e esquematizá-las num mapa de rede.
Com base numa solução de gestão distribuída permite facilmente encontrar causas de falhas na rede, capaz de automaticamente realizar um inventário de dispositivos, identificando os sistemas críticos, armazenando toda a informação sobre a topologia de rede e a informações de eventos numa base de dados interna.
Esta plataforma é composta por um conjunto de módulos diversificados, dos quais se destacam os seguintes:

- Servidor de Eventos – responsável por manipular todos os eventos do sistema distribuído;
- Consola de Eventos, fornece a interface gráfica com o utilizador, quer seja através de uma aplicação Java ou de uma versão Web, permitindo visualizar todos os eventos do sistema;
- Servidor *NetView*, o servidor é uma parte central nas tarefas de gestão da rede que utiliza o SNMP para descobrir, monitorizar e configurar redes TCP/IP.

O conjunto de módulos *NetView* fornece uma ferramenta de gestão de eventos de rede, que incluem eventos de status, eventos limites de colecta de dados SNMP e eventos de isolamento de falha de activos de rede. Tem a capacidade de fornecer relatórios de dados recolhidos e estatísticos.

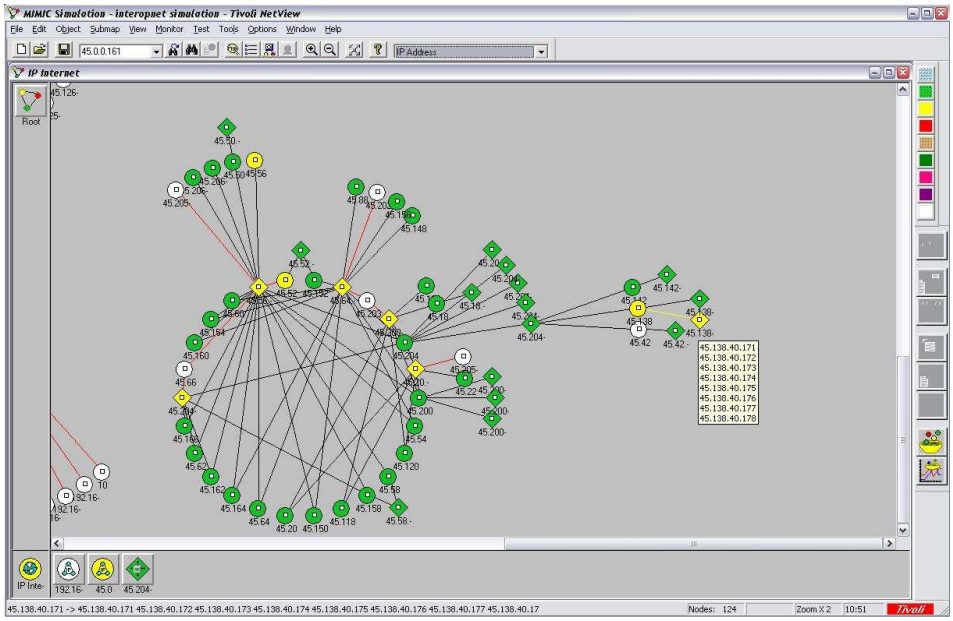

Figura 3.2 - IBM Tivoli NetView

Esta plataforma também permite a integração com outras aplicações, tais como:

- CiscoWorks2000;
- *nGenius Performance Manager*;
- *Xerox CentreWare*;
- *3Com Enterprise Management Suite*;

O *Tivoli NetView* e o seu vasto leque de aplicações, apresentam-se como uma solução integrada que pretende dar resposta a todas as áreas de gestão, oferecendo estatísticas e gráficos de desempenho e relatórios dos itens inventariados, como dispositivos de redes e computadores, embora neste caso, apenas o hardware.

3.3.3. MICROSOFT SYSTEM CENTER CONFIGURATION MANAGER

Anteriormente chamado de *Microsoft System Managment Server* (SMS) é um programa de gestão de sistemas *Windows*, desenvolvido pela *Microsoft* [19]. Através deste programa é possível realizar o controlo remoto, gestão de actualizações, distribuição de software, bem como o inventário de software e hardware.

O SMS passou a *Microsoft System Center Configuration Manager* (SCCM) em 2007, na sétima versão desta aplicação, Figura 3.3. Com as mesmas funcionalidades do SMS 2003 SP3, acrescenta a integração com o *Windows Serve*r 2008, bem como com o *Windows Vista*. Foram

ainda adicionadas novas ferramentas de gestão (dispositivos móveis, *update* de software) e de segurança (*Network Access Protection*).

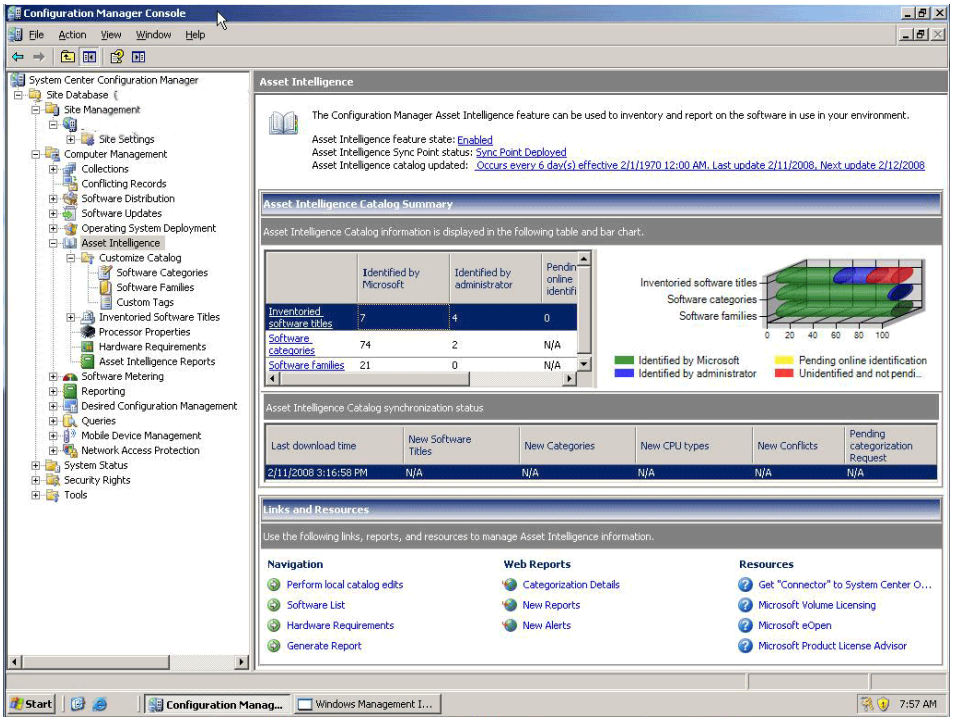

Figura 3.3 - Microsoft System Center Configuration Manager

O SCCM corre sobre o sistema operativo *Windows* e apenas suporta clientes com este sistema operativo – pelo menos de forma a poder tirar todo o partido das funcionalidades oferecidas. Com uma plena integração com um servidor *Active Directory* (*Microsoft*), o SCCM permite também gerir utilizadores e grupos, políticas de grupo e de utilizadores (*group policies*), perfis remotos (*roaming profiles*) e cotas de espaço em disco (*disk quotas*).

É possível também usar esta ferramenta (ou conjunto de ferramentas) para controlar a infra-estrutura de activos, mantendo uma monitorização constante, sobre o estado e o uso desses mesmos activos.

Além da integração com o *Active Directory*, a ultima versão do *Configuration Manager*, integra-se também com outros produtos da *Microsoft*, nomeadamente com o *Microsoft Office 2007*, o *Windows Vista*, o *Windows Server 2008* e com o *Microsoft Exchange Server 2007*, de forma a alcançar uma solução única e abrangente de gestão de sistemas.

Concluindo, o SCCM apesar de ser apenas voltado para a gestão de máquinas (descurando a infra-estrutura de rede) é uma ferramenta de gestão que permiti aumentar a eficiência, reduzindo as tarefas manuais. Com o *Configuration Manager* consegue-se um departamento de TI eficiente, implementando instalações e actualizações de uma forma rápida, e simultaneamente facilitando a implementação de configurações em todo o parque informático. Capaz de realizar *auto-discover*, recolhe informações estatísticas das máquinas monitorizadas através de SNMP.

Como aspecto negativo destaca-se o facto de não suportar outros sistemas operativos para além do sistema operativo *Microsoft Windows*.

3.3.4. OPENNMS

O *Open Network Managment System* (*OpenNMS*) é um projecto *Opensource* dedicado à gestão de redes [20]. Criado inicialmente em 2004 é escrito em *Java* e suportado pela quase totalidade dos sistemas operativos (*Linux*, *Windows*, *MacOS* e *Solaris*).

Esta ferramenta de gestão fornece funcionalidades de monitorização de disponibilidade, aquisição de dados de performance, gestão de eventos e notificações. Além disso disponibiliza o *auto- discover* de activos bem como a integração com outros produtos.

De forma a competir com ferramentas pagas, como o *HP Openview* ou *Tivoli Netview*, a versão 1.6.0, Figura 3.4, trouxe notórias inovações em quatro áreas principais: *auto-discover*; gestão de eventos; recolha de dados de performance e serviços de monitorização.

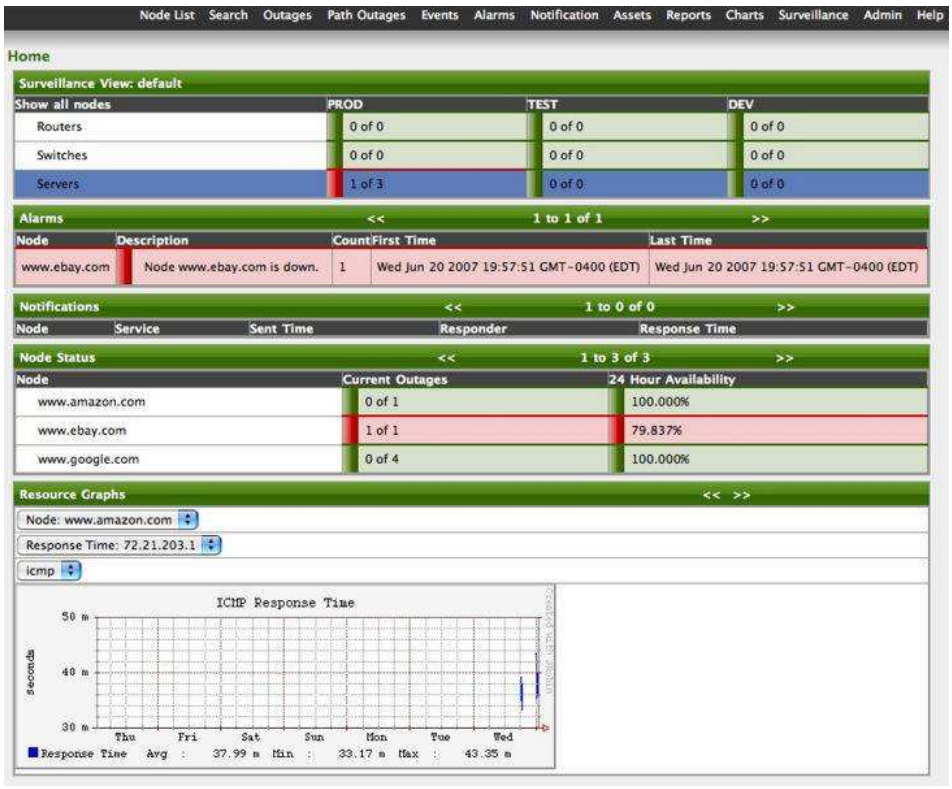

Figura 3.4 - OpenNMS

Com interface gráfica Web, fornece uma forma de visualizar o estado dos serviços e interfaces de rede, a disponibilidade dos serviços, os eventos gerados, gráficos de desempenho ou informação sobre equipamentos. Através de controlo de acessos, é possível aceder ao sistema como administrador, dando a possibilidade de gerir utilizadores e grupos, notificações de eventos ou serviços monitorizados e solicitar relatórios de disponibilidade.

A funcionalidade de *auto-discover* nesta aplicação está bem desenvolvida, permitindo que sejam descobertos serviços activos como por exemplo: SNMP, SMTP, SMB, POP3, TCP, ICMP, *Microsoft Exchange*, DNS, LDAP, HTTP, DHCP, IMAP, ou FTP. Esta funcionalidade por defeito é executada a cada 24 horas.

A Monitorização também suporta diversos protocolos e serviços a destacar:

- Web: HTTP e HTTPS;
- *Mail*: *POP3*, *IMAP* e SMTP;
- Base de Dados: *Oracle*, *Sybase*, *Informix*, *SQL Server*, *MySQL*, *Postgres*;
- Rede: ICMP, SNMP, DNS, DHCP, FTP, SSH e LDAP;
- Outros: *Citrix* e *Lotus Domino IIOP*.

Demais serviços podem facilmente ser configurados, introduzindo nome do serviço e respectivo porto.
O *OpenNMS* fornece também relatórios, estatísticas e gráficos de desempenho.
Os dados estatísticos que podem ser obtidos são diversos, dos quais se destaca:

- Utilização;
- Bytes entrada e saída (*in*/*out*);
- Erros entrada e saída (*in/out*);
- Descartes entrada e saída (*in/out*);
- Utilização da UCP;
- Memória disponível;
- Falhas de *buffers*;
- Distribuição de protocolos entrada e saída (*in/out*);
- Percentagem de *buffer hits*;
- Perda de *buffers*.

Além destes valores, há a possibilidade de se gerar outros gráficos baseados em variáveis SNMP, configurando-os manualmente.

Na figura seguinte, Figura 3.5, apresenta-se um exemplo de um gráfico de tráfego de um *switch*, filtrado por rede virtual (VLAN), distinguindo quantidade de bits de entrada e saída (*in/out*).

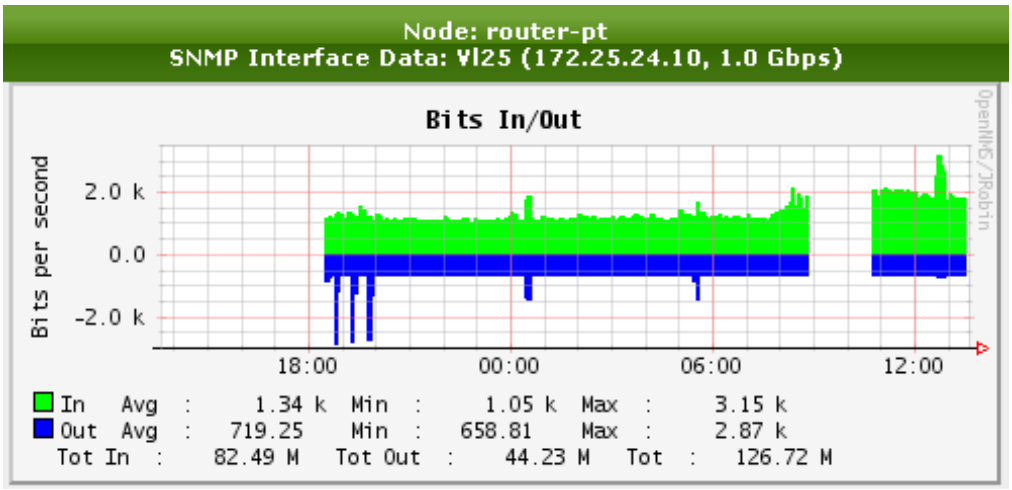

Figura 3.5 - OpenNMS - Exemplo Gráfico

3.3.5. LANDESK MANAGEMENT SUITE

Esta ferramenta permite gerir hardware e software com facilidade [21]. Com o *Landesk Management Suite* é possível gerir todos os sistemas clientes com eficiência, desde as tarefas de gestão de segurança até à actualização e protecção de *Desktops*, servidores ou mesmo dispositivos móveis, através da distribuição e actualização automática de aplicações.

A *Avocent,* vendedora desta aplicação, garante o aumento da eficiência, a redução do tempo de gestão e a redução dos custos associados às tarefas de *helpdesk*.

Inicialmente criado (1985) como *LAN Systems*, este produto foi adquirido pela Intel em 1991, formando uma divisão própria. Em 2002 tornou se um empresa independente sendo comprada pela *Avocent* em 2006.

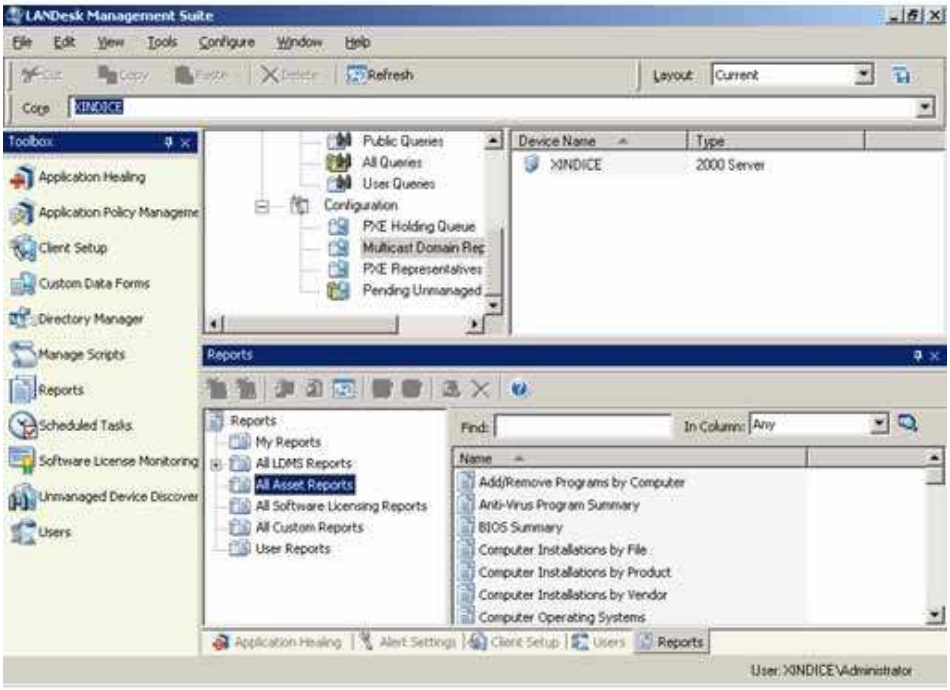

Figura 3.6 - Landesk Management Suite

Actualmente na versão 8.8, Figura 3.6, fornece uma solução de gestão para todas as empresas, combinando as funcionalidades de gestão de activos, distribuição de software ou controlo remoto.

As principais funcionalidades são:

- Gestão de activos;
- Distribuição de software;
- Descoberta automática de dispositivos;
- Gestão de inventário;
- Migração de sistemas;
- Migração de perfis;
- Controlo Remoto;
- Monitorização de licenças de software;
- Relatórios abrangentes, gráficos de desempenho e estatísticas.

Esta ferramenta permite a integração com outras aplicações, como por exemplo o *Remedy* ou o *ThinkVantage* da IBM.

3.3.6. SPICEWORKS

O *Spiceworks* é uma ferramenta simples mas poderosa, Figura 3.7. Com uma interface web, multi-utilizador, permite inventariar, monitorizar, criar relatórios e verificar problemas na rede informática [22]. Em paralelo possui um sistema bastante desenvolvido de "*trouble tickets*" (*Helpdesk*/Suporte Local), além de integrar na mesma interface uma comunidade grande de profissionais de TI, que trocam experiências e informação.

A empresa que oferece esta ferramenta, disponibiliza-a de forma gratuita mantendo algumas formas de donativos, bem como uma estreita ligação com marcas tecnológicas, quer seja através de publicidade integrada ou informação sobre produtos.

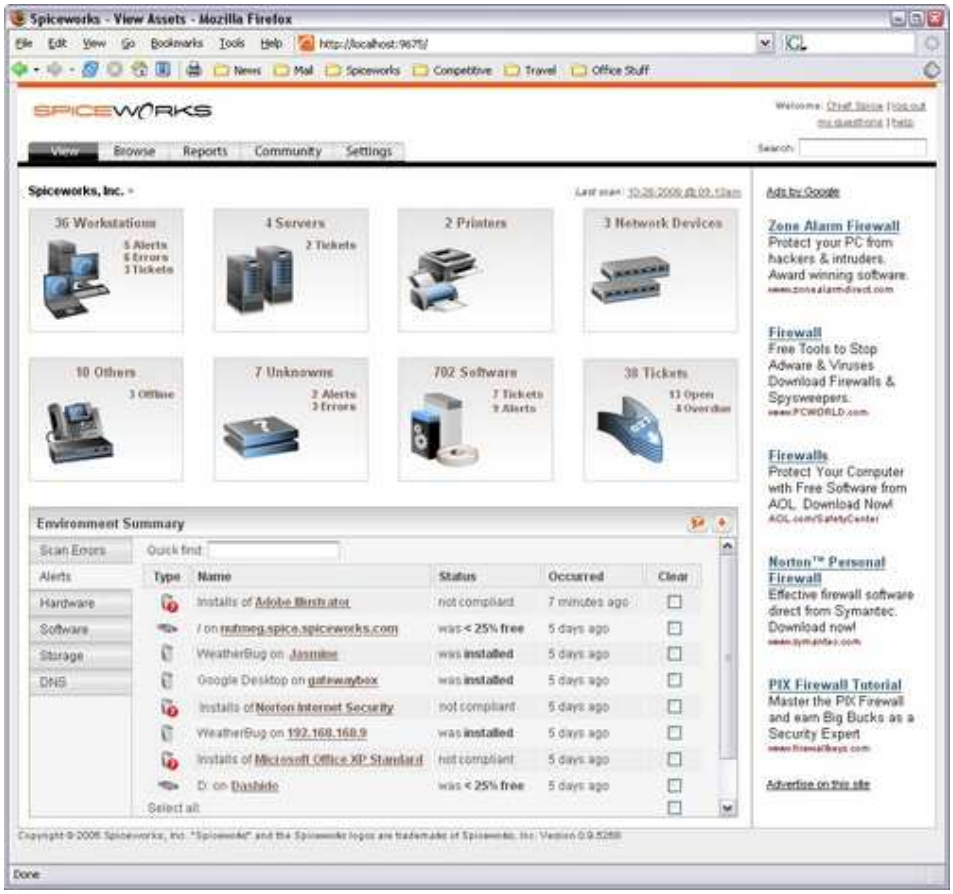

Figura 3.7 - Spiceworks

Os pontos principais que o *Spiceworks* foca são:

- Descoberta de dispositivos;
- Gestão de inventário;

- Gestão de suporte local;
- Controlo remoto (integrado com Ligação ao Ambiente de Trabalho Remoto da *Microsoft*);
- Relatórios;
- Alertas.

Após a instalação e a configuração das definições globais (utilizadores, *mails*) define-se a gama de endereços que devem ser monitorizados. A versão 4.1 consegue detectar correctamente máquinas com sistemas operativos *Windows*, *MacOS* e *Linux*, bem como muitas das suas características, tais como utilizadores, software instalado, impressoras, espaço em disco, etc. através de SNMP. Os dados recolhidos são disponibilizados em relatórios, estatísticas e gráficos de desempenho. Ao nível da rede, a ultima versão deste produto testada, passou a incluir um mapa de rede.

3.4. ANÁLISE COMPARATIVA

A análise das várias plataformas disponíveis é um trabalho difícil e subjectivo. Paralelamente, o facto de não ser possível efectuar uma avaliação prática das várias plataformas e durante um período de tempo suficiente para serem obtidas conclusões fidedignas, resta fazer-se uma análise teórica das funcionalidades oferecidas por cada uma delas. Com esta análise procura-se encontrar a solução que melhor se adeqúe às reais necessidades do caso em estudo.
As plataformas e aplicações de gestão, descritas anteriormente, não possuem significativas vantagens competitivas quando comparadas umas com as outras, uma vez que, todas implementam as normas de gestão actuais e um conjunto de funcionalidades semelhante.
Existem, no entanto outros factores a ter em contar, tais como, a relação funcionalidade/preço, a facilidade de implementação ou a quantidade/qualidade de informação disponibilizada.
De forma a facilitar a análise comparativa das plataformas estudadas foi construída uma tabela resumo das várias características, Tabela 3.2.

Todas as plataformas estudadas são possíveis soluções para aplicar a diversos cenários reais. A escolha, de cada uma delas, passa pela especificidade de cada cenário, assim como pelos objectivos de gestão em cada um deles.
Todas as plataformas apresentam pontos fortes e algumas lacunas ou aspectos menos explorados, mas que não comprometem o seu funcionamento ou valor real.

		Sistemas de Gestão					
	Sistemas → Funcionalidades ↓	**HP Open View**	**IBM Tivoli NetView**	**Microsoft SCCM (ex SMS)**	**OpenNMS**	**LanDesk Man. Suite**	**Spiceworks**
Sistema	SO suportados instalação	todos		win	*nix	win	todos
	Interface com utilizador (GUI/Web)	web gui	web gui	gui	web	web	web
	Integração com outras aplicações	S	S	N	S	S	lim [1]
	Estatísticas	S	N	S	S	S	S
	Gráficos de desempenho	S	S		S	S	S
	SNMP	S	S	S	S	N	S
	Envio de alertas	S		N	S	S	S
	Relatórios	S	S	N	S	S	S
Gestão Redes	Auto discover	S	S	N	S	S	S
	Gestão de equipamentos	S	S	N		S	S
	Monitorização remota (RMON)	S	S		S	N	N
	Processamento de eventos	S	S	N	S	N	S
	Mapa de rede	S	S	N	N	N	S
Gestão Sistemas	Auto discover	S	S	S	S	S	S
	Distribuição de software	N	N	S	N	S	N
	Gestão de politicas	N	S	S	N	S	N
	Inventário (HardWare e SoftWare)	N	hw	hw/sw	hw/sw	hw/sw	hw/sw
	Controlo remoto	N		S	N	S	S [2]
	Controlo de licenças	N		S	N	S	S [3]
	SO suportados gestão	todos	todos	win	todos	todos	todos
Preço		$4995	$1000	$579	0 €	$89 [4]	0 €

Tabela 3.2 - Comparativo Sistemas de Gestão

Da análise comparativa efectuada pode-se constatar que umas aplicações apresentam como vantagem a possibilidade de integração com outras aplicações, outras o profundo conhecimento dos sistemas geridos, ou ainda as inúmeras funcionalidades disponibilizadas.

[1] Limitado - Apenas desencadeia chamadas a outras aplicações
[2] Microsoft Remote Desktop
[3] Através de plugins
[4] $89 por nó (mínimo 10 nós) $499 por servidor)

No entanto, todas as plataformas descritas anteriormente representam uma possível escolha para aplicar ao cenário em estudo, podendo eventualmente apenas serem distinguidas pelo factor económico.

Por tudo que foi exposto neste capítulo podemos concluir que a preferência por uma determinada plataforma deve ter em conta os requisitos específicos da infra-estrutura. Procurando encontrar as funcionalidades que melhor se adaptam às necessidades do caso real.

4. ESTUDO DE UM CASO

4.1. INTRODUÇÃO

Como já foi referido anteriormente, uma gestão efectiva terá de ser baseada no conhecimento profundo dos mecanismos de gestão, das tecnologias envolvidas, da configuração da infra-estrutura e da orgânica da instituição.

Para implementar um sistema de gestão adequado a um cenário real é necessário efectuar o estudo das tecnologias e plataformas de gestão de redes e sistemas, seguido da análise prática das suas potencialidades num cenário real, procurando encontrar as funcionalidades que melhor se adaptam às necessidades do cenário em questão.

Para tal, é necessário caracterizar a organização em questão, a Rádio e Televisão de Portugal do Norte – RTP, e a sua infra-estrutura informática.

Assim, neste capítulo será abordada a organização da RTP Porto e da sua infra-estrutura informática, assim como serão enumeradas as reais necessidades de gestão.

4.2. A RTP - RÁDIO E TELEVISÃO DE PORTUGAL

A RTP é uma empresa de capitais públicos, fundada em 1935 com o nome de Emissora Nacional. Em 2004, foram reestruturadas e fundidas as duas empresas RTP – Radiotelevisão Portuguesa e RDP – Radiodifusão Portuguesa, numa única empresa pública, a Rádio e Televisão de Portugal.

Actualmente a RTP além da sua sede em Lisboa, conta com delegações por todo o país e ilhas - Viana do Castelo, Vila Real, Viseu, Guarda e Castelo Branco, Faro, Évora, Coimbra, Bragança, Açores e Madeira – e com um Centro de Produção em Vila Nova de Gaia – a RTP Porto.

No Centro de Produção Norte (CPN), são produzidas em média treze (13) horas de emissão diária para os canais RTP1 e RTPn, e cerca de dez (10) horas diárias para vários canais da RDP (Antena1, Antena2 e Antena3). Trabalham cerca de quatrocentas (400) pessoas, sendo que algumas delas, com funções de apoio directo à emissão trabalham por turnos, durante vinte e quatro (24) horas por dia, sete (7) dias por semana.

4.3. O SISTEMA DE INFORMAÇÃO ACTUAL

O Sistema de Informação no CPN é um sistema complexo, e com exigências grandes ao nível da disponibilidade, uma vez que se trata de um sistema crítico de apoio à actividade principal da empresa.

Além dos comuns sistemas de informação de contabilidade, sistema de gestão de frotas, gestão de pessoal, existem inúmeros sistemas específicos directamente ligados à produção e emissão de televisão e rádio.

O parque informático é composto por uma grande variedade de equipamentos, que apesar de diferentes níveis de importância, devem ser monitorizados por igual.
Na tabela seguinte, Tabela 4.1.,são apresentados os sistemas que constituem a infra-estrutura.

Servidores	Domínio
	Ficheiros
	Comunicações
Postos de Trabalho	Escritório
	Ilhas de Edição
	Outros
Comunicações de Dados	CPN – Routers e Switchs
	Routers Delegações Norte
Comunicações de Voz	Central Telefónica Ericsson
	Central Telefónica Cisco Call Manager
Equipamentos de Rede	Multifunções, Impressoras, Faxes
	Terminais Biométricos de Controlo de Acesso
Vídeo Vigilância	Câmaras
	Gravadores

Tabela 4.1 - Sistema de Informação Actual

Os servidores estão maioritariamente assentes em *Windows Server*, havendo uma minoria insignificante de sistemas que não pertencem à família *Microsoft*.
Relativamente aos postos de trabalho podemos considerar que são praticamente todos da família *Windows*, sendo dentro desta família a maioria na versão XP. Os postos de trabalho restantes consistem em sistemas proprietários com funções específicas, tais como, órgão de luzes, mesas de mistura áudio e vídeo, teleponto, etc.

4.3.1. SISTEMAS

No centro de emissão do Porto, os sistemas existentes são em número reduzido, uma vez que a maioria dos servidores aplicacionais estão centralizados na sede – Lisboa. Existem, no entanto servidores de ficheiros, fax, controlador de domínio, e computadores de apoio a sistemas paralelos, como a central telefónica ou vídeo vigilância.
A tecnologia utilizada para suportar os vários sistemas é baseada na família *Windows*, com especial incidência na versão 2003 *Server* deste sistema operativo. Existem ainda servidores com o sistema operativo *Linux*, com funções de servidor de Fax ou tarefas auxiliares na gestão da rede.
O sistema de informação comunica apenas com delegações RTP, do norte do país e com o edifício sede em Lisboa, sendo através da intra-estrutura de Lisboa que são feitas as ligações para as restantes delegações e ao mundo exterior – a Internet.

4.3.2. A INFRA-ESTRUTURA DE COMUNICAÇÕES DE DADOS

A infra-estrutura de comunicação de dados em funcionamento no CPN da RTP é composta maioritariamente por tecnologias e equipamentos *standard*, pelo que não é necessário ter em conta nenhuma especificação especial.

Composta na quase totalidade por activos de rede da marca Cisco, tem como meios físicos de transmissão, cablagem UTP Cat.6 e Fibra Óptica Multimodo.

Organizado logicamente com uma topologia em Estrela, mais especificamente Estrela Estendida, a rede de comunicações estende-se por cinco (5) edifícios, sendo a velocidade de comunicação 1Gbps, Figura 4.1.

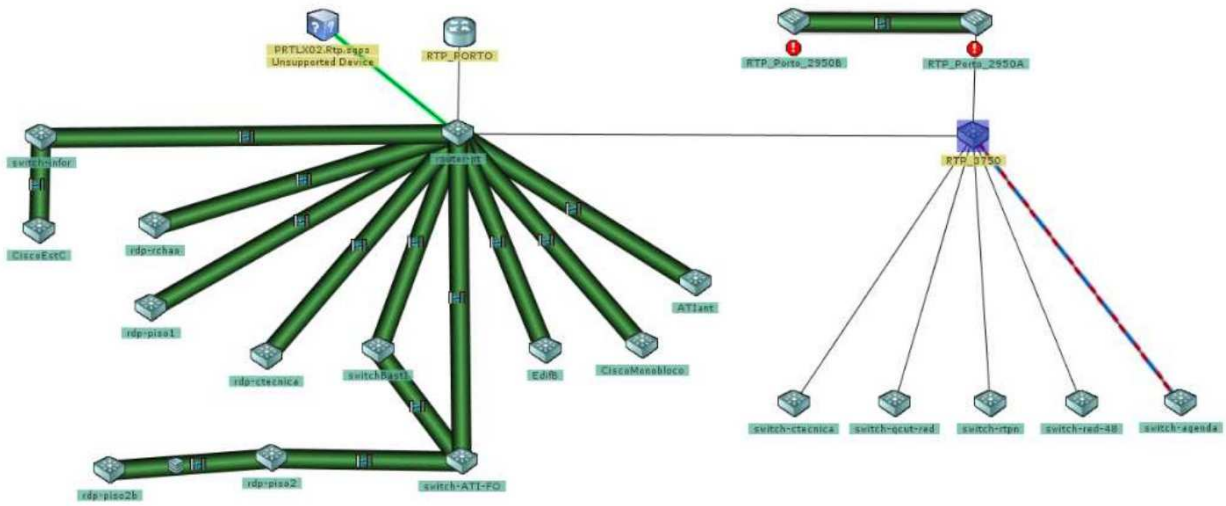

Figura 4.1 - Esquema de Rede Dados (CNA)

A nível lógico existem definidas quatro (4) VLANs que albergam diferentes áreas, nomeadamente informação, produção, administrativa, apoio e vídeo vigilância.

Do CPN existem ligações de dados para a RTP Lisboa e delegações do norte do país, concentradas num equipamento proprietário do *Internet Service Provider* (ISP).

As redes utilizadas dentro das instalações do Porto são:

- 200.0.2.0 /24;
- 192.168.12.0 /24;
- 172.25.24.0 /21;
- 192.168.130.0 /24.

Além destas redes nas delegações da Rádio e Televisão, sediadas no norte do país (ou sobre a alçada da equipa de informática da RTP Porto) constam as seguintes redes:

- Viana do Castelo: 172.25.248.0 /21;
- Viseu: 172.25.240.0 /21;
- Guarda: 172.25.232.0 /21;
- Bragança: 172.25.224.0 /21;
- Vila Real: 172.25.216.0 /21;
- Castelo Branco: 172.25.208.0 /21.

Com o sistema existente (prévio a este estudo) não existem dados que permitam analisar a saturação de pontos de rede ou tipo de tráfego nos *links*. Dado a actividade principal da RTP ser a difusão de notícias é primordial que os acessos estejam sempre disponíveis, assim como garantir as velocidades necessárias para o correcto desempenho da actividade.
O acesso à Internet é realizado através de *proxies* situados em Lisboa, e administrados pela equipa de Sistemas da sede, não havendo qualquer controlo sobre os mesmos na RTP Porto.

4.3.3. MONITORIZAÇÃO ACTUAL

No CPN já existia um sistema de apoio à monitorização – *Spiceworks* versão 3.6.33156.
Este sistema de monitorização, instalado há cerca de ano e meio, oferece uma visão global dos equipamentos de rede, desde computadores, impressoras ou activos de rede, tais como *switchs* ou *routers*.
Instalado inicialmente numa máquina comum, ou seja sem nenhuma característica especial, com o objectivo de serem feitos testes para explorar as suas potencialidades, rapidamente foi transferido para uma máquina com características acrescidas.
Numa primeira análise feita às potencialidades da aplicação constatou-se que os pontos fortes desta aplicação são: a simplicidade de instalação e configuração; a quantidade de nós de redes descobertos com sucesso e quantidade/qualidade da informação recolhida, principalmente de máquinas *Windows*, que constituem a quase totalidade do parque informático actual.
Relativamente à informação recolhida das máquinas com sistema operativo *Windows* é de destacar:

- Hardware Base (processador, memória, placa de rede);
- Disco (totalidade e quantidade disponível);

- Anti-vírus (disponibilidade e se actualizado);
- Software (aplicações instaladas e versão, bem como informação sobre disponibilidade de novas versões online);
- Serviços (instalados e em execução);
- Contas de utilizadores;
- Impressoras (instaladas e quantidade de tinteiro/toner).

Esta ferramenta também disponibiliza relatórios exaustivos, sobre todos os parâmetros monitorizados, bem como sistema de alarmes baseado em métricas definidas pelo utilizador.
Os relatórios disponibilizados dividem-se em dois tipos: resumos estatísticos disponíveis para as variáveis mais comuns do sistema e relatórios detalhados e personalizáveis. Sendo de salientar que esta informação aparece de uma forma gráfica.
Os relatórios detalhados, apesar de menos atractivos, são aqueles que fornecem dados realmente importantes para a gestão da área tecnológica.
Na instalação base já existe um conjunto de relatórios padrão, para as necessidades mais comuns, sendo alguns deles “PCs sem Anti-Vírus”, “Uso do espaço em disco” ou “Aplicações instaladas por PC”.
Além destes, é possível adicionar um qualquer relatório, seja disponibilizado pela comunidade e importado para o sistema, seja através da sua criação de raiz, recorrendo a uma ferramenta gráfica disponibilizada ou, para relatórios mais complexos, através de instruções SQL. Trata-se portanto de uma óptima ferramenta para a inventariação, gestão e monitorização do parque informático.
No entanto, apenas recolhe informação diversificada dos postos de trabalho, deixando de fora, informação detalhada relativa aos activos de rede, ou equipamentos específicos, como por exemplo terminais biométricos, vídeo vigilância ou determinadas impressoras de rede.
Outro aspecto crítico, ao qual esta aplicação não é capaz de dar resposta, é ao nível dos *links* de rede onde é requerida uma monitorização constante da largura de banda, tráfego ou erros.

4.3.4. REQUISITOS DA SOLUÇÃO

A plataforma a construir deverá contemplar a gestão de redes e sistemas, providenciando os mecanismos mais rudimentares de construção de mapas, recolha de estatísticas de tráfego/máquina, envio de alertas, facilidades de integração com outras aplicações, inventariação de software e hardware, distribuição de software, controlo remoto e suporte das normas em vigor nos sistemas de gestão. Sendo a infra-estrutura constituída, na sua maior parte, por

equipamento da marca Cisco, deverá ser acautelada a possibilidade de gerir este equipamento remotamente, retirando dele o maior partido possível.

4.3.5. MONITORIZAÇÃO

A necessidade de monitorizar e gerir as TI de uma forma global facilita a detecção rápida de erros e, ao mesmo tempo, permite a análise dos seguintes pontos: fiabilidade; avaliação de performance; integridade e segurança.

O objectivo de um projecto deste género é, antes de mais, criar uma visão integrada de todo o SI. Esta visão, documentada através de esquemas, tabelas ou diagramas, deve ser capaz de transmitir em tempo real, o estado actual de todos os equipamentos e serviços monitorizados. Baseado na esquematização e num sistema global de Gestão, o sistema deve ser capaz de alertar para variáveis que se desviem dos valores padrão, capaz de disparar alertas para eventos críticos, e permitir desencadear as acções correctivas que permitam a reposição e configuração do sistema.

Embora teoricamente tudo possa ser monitorizado e analisado, esta não é a solução mais indicada, pois além de se criar um sistema demasiado complicado, dada a dimensão dos dados recolhidos, nem tudo merece a mesma atenção.

Alguns dos sistemas monitorizados terão atenção especial, sendo analisados todos os serviços e variáveis de estado (espaço em disco, memória, etc.), enquanto que em outros equipamentos (Impressoras, por exemplo) apenas será verificado o seu estado global (OK ou Erro).

Pelo que, para este cenário concreto, pretende-se um sistema capaz de recolher dados, de todos os equipamentos em funcionamento, independentemente da marca, modelo e do tipo de equipamento em causa.

O sistema a implementar deverá ser capaz de monitorizar a disponibilidade da rede e dos recursos, recolher variáveis de estado, centralizar registos de eventos (SNMP *Traps* ou *Logs*/Eventos) e ser capaz de enviar alertas no caso de acontecerem falhas críticas.

A monitorização a ser feita está apresentada de uma forma sumária na tabela seguinte, Tabela 4.2.

Existem várias soluções proprietárias que disponibilizam muita informação sobre os equipamentos, no entanto, trata-se de soluções simples e focadas apenas em parte do problema, quando o que se pretende é obter um sistema único, capaz e abrangente.

CATEGORIA	OBJECTIVOS MONITORIZAÇÂO
Servidores	• Estado • Serviços • Espaço em Disco • Eventos
Postos de Trabalho	• Estado • Espaço em Disco • Versões de Software
Comunicações Dados (*Routers* e *Switchs*)	• Estado • Carga de Processamento • Falha de Comunicações • Eventos
Comunicações Voz (*Ericsson* e *Cisco Call Manager*)	• Disponibilidade • Eventos
Equipamentos de rede (Multifunções, Impressoras, Faxes, Terminais Biométricos)	• Disponibilidade • Eventos

Tabela 4.2 - Monitorização

4.3.6. GESTÃO DE ACTUALIZAÇÕES

A gestão de actualizações não sendo uma tarefa crítica para o desenrolar de actividades numa empresa, é bastante primordial, uma vez que este tipo de tarefas, não automatizada, ocupa demasiado tempo dos técnicos informáticos.

A gestão de actualizações assente em duas fases distintas. A primeira trata-se de manter uma base de dados com todo o software instalado em todas as máquinas, bem como a respectiva versão instalada. Esta informação é útil para comparar com as ultimas versões disponíveis de cada software, de forma a detectar computadores com aplicações ou serviços desactualizados.

A segunda fase de uma correcta gestão de actualizações, é automatizar o processo de distribuição automática de actualizações em todo o parque informático.

Manter os computadores de toda a empresa actualizados é um factor decisivo para o desenrolar das actividades com eficiência [23]. Por um lado, cada utilizador deverá poder trabalhar com a versão mais recente de cada aplicação, o que implica, mais e melhores funcionalidades e menos *bugs* na sua execução. Por outro lado, o sistema operativo deverá estar actualizado ao nível das protecções de segurança. Praticamente todos os dias, são detectadas novas falhas, que não corrigidas podem comprometer a máquina, levando à perda de informações.

No Centro de Produção da RTP Porto, a inventariação das aplicações instaladas e respectiva versão, está a cargo da aplicação *Spiceworks* (descrito no Capitulo 4.3.3), com sucesso assinalável. A capacidade de recolher informações das máquinas é bastante elevada e associada aos relatórios personalizáveis, permite que a qualquer momento, se possa analisar o estado actual do software, através de uma visão global.

Uma funcionalidade importante, mas inexistente na solução *Spiceworks*, é a capacidade de distribuir, de forma automática, versões actualizadas das aplicações e nas várias máquinas. Para ultrapassar esta limitação foram utilizadas várias aplicações proprietárias para cada uma das necessidades que iam surgindo.

4.3.7. GESTÃO DE ACTIVOS DE REDE

Uma rede informática refere-se a vários computadores ou outros equipamentos, interligados entre si, através de um sistema de comunicações com o objectivo de partilhar dados, impressoras, mensagens, etc. Estas redes informáticas são hoje em dia fundamentais para o desenvolvimento da actividade de negócio de qualquer empresa, e a Rádio e Televisão de Portugal não é excepção, com a agravante de que uns dos principais focos de trabalho – as notícias – requerer que os dados estejam disponíveis onde são precisos no mais curto espaço de tempo. Por este motivo a rede de dados tem de ter um desempenho acima da média e uma disponibilidade de 100%.

A infra-estrutura de rede de toda a RTP sofreu recentemente uma profunda alteração, passando a ser praticamente toda ela suportada por activos da marca Cisco, e por essa razão optou-se por explorar também as soluções de gestão do fabricante juntamente com outras plataformas de gestão generalista. A escolha recaiu, com naturalidade, no *Cisco Network Manager* (CNA), Figura 4.2, uma vez que este permite uma visão global de todos os activos e uma gestão centralizada da infra-estrutura de comunicações física e lógica.

O CNA além de centralizar a gestão das configurações de *switchs*, *routers*, simplifica outras tarefas de gestão, tais como actualização do *firmware*, realizar cópias de segurança das configurações, monitorização de variáveis de estado ou envio de alertas.

O CNA é, de facto, a ferramenta mais completa quando se trata de gerir activos desta marca de equipamentos, pecando apenas por se limitar à marca e não ser possível integrar todas as funcionalidades fornecidas com outras plataformas de gestão.

Actualmente a versão 5.3 em uso, possui como principais funções a configuração de equipamentos e a monitorização de *links*. Esta versão não possui ainda suporte para *Access Points* e central telefónica VOIP da Cisco (*Cisco Call Manager*), em uso na RTP Porto.

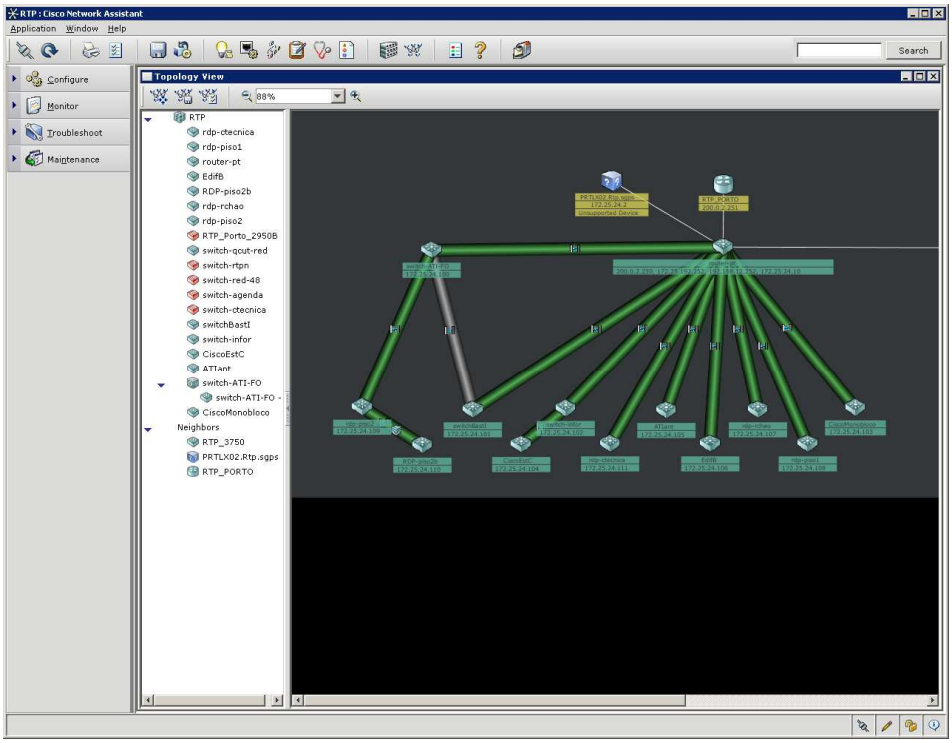

Figura 4.2 - Cisco Network Assistant

5. IMPLEMENTAÇÃO DE UMA SOLUÇÃO

5.1. INTRODUÇÃO

De tudo que foi exposto até aqui, a escolha da plataforma pode ser uma tarefa complexa, já que a oferta é muita, as funcionalidades semelhantes e em muitos casos os preços também idênticos.

No entanto, a plataforma deverá apresentar um custo competitivo tendo em conta as funcionalidades oferecidas, assim como as condições de suporte técnico e a facilidade de implementação.

Neste capítulo será estudada, com algum pormenor, a aplicação sobre a qual recaiu a escolha para constituir a plataforma de gestão. Esta escolha teve em conta vários factores, dos quais se destacam as seguintes funcionalidades: a facilidade de operação; o custo e a adaptabilidade ao caso real, a RTP Porto.

5.2. A PLATAFORMA OPENNMS

A plataforma *OpenNMS* foi a eleita. As razões que levaram a esta escolha são principalmente duas: a quantidade de funcionalidades oferecidas e o custo.

De entre as aplicações estudadas, o *OpenNMS* encontra-se entre aquelas que mais funcionalidades oferecem na sua versão base, permitindo ainda ser integrado com outras aplicações de forma a estender as suas capacidades. Relativamente aos custos, esta é sem dúvida a solução mais apelativa. Sendo distribuída sob a licença GPL (GNU *Public License*), representa para o utilizador final custo zero (além de outros direitos, como o direito à alteração ou distribuição do software).

O *OpenNMS*, escrito em Java e com uma interface Web com o utilizador, fornece um auxílio extra às tarefas de gestão e configuração de rede e dos sistemas administrados. Desde análises simples, como *uptime* ou carga da máquina, até análises mais complexas como tráfego (quantidade, protocolo) ou utilização do *buffer*.

A implementação de uma plataforma de gestão potencia um melhor aproveitamento dos recursos de rede, trazendo uma fiabilidade e disponibilidade acrescida aos serviços suportados. Neste campo o *OpenNMS* oferece uma série de funcionalidades que permitem passar de uma gestão reactiva para uma gestão activa, através da monitorização constante dos objectos da rede, possibilitando uma visão centralizada do estado e da topologia da infra-estrutura em qualquer instante. Esta monitorização é complementada com um sistema de eventos e alertas que garantem uma resposta rápida e eficaz por parte do gestor.

Outro factor, tido em conta, é o facto de se tratar de uma plataforma independente, o que facilita a integração de MIBs SNMP de vários fornecedores. A utilização de uma MIB privada numa solução SNMP de outro fornecedor, não é normalmente, uma função simples.

5.2.1. AS FUNÇÕES DE GESTÃO OPENNMS

As funcionalidades oferecidas por esta aplicação que consideramos importantes para o caso de estudo são (independentemente da ordem): descoberta automática dos objectos de rede, monitorização constante de activos de rede e respectivos serviços; envio de alertas baseados em condições pré-definidas e gestão de objectos SNMP.

O *OpenNMS* é um projecto recente (2004) e ainda em desenvolvimento, pelo que espera-se a curto prazo a disponibilização de novas funcionalidades, assim como melhorias significativas às já existentes. Por outro lado, tratando-se de um projecto desenvolvido sobre a licença GNU, existem a nível mundial inúmeros programadores a desenvolver as funcionalidades oferecidas por esta ferramenta.

A ferramenta de gestão *OpenNMS*, embora bastante completa, não cumpre com o mesmo detalhe as cinco áreas funcionais propostas pela ISO - FCAPS.

As duas principais áreas cobertas pela aplicação *OpenNMS* são a Gestão de Falhas e Gestão de Desempenho.

A Gestão de Falhas é realizada de uma forma muito exaustiva, recorrendo a três mecanismos diferentes: *service polling*, recepção de mensagens SNMP (SNMP *traps*) e definição de limites comparados com os dados recolhidos.

Na gestão de Performance também são utilizados diferentes mecanismos de recolha de informação de forma a criar uma imagem completa do desempenho de cada máquina ou serviço. Esses mecanismos são o *Service Collector*, o SNMP, o JMX, o protocolo HTTP e o *NSClient*.

As três áreas funcionais restantes do modelo FCAPS são, de certa forma, consideradas pela aplicação, mesmo que não na sua totalidade, ou recorrendo à interligação com outras aplicações.

A Gestão de Contabilidade de Utilização é parcialmente implementada, uma vez que, os dados relativos ao uso da rede, ou à utilização do processador ou espaço em disco são recolhidos por esta ferramenta. Estes dados não são utilizados directamente na Contabilidade de Utilização, mas podem ser exportados para sistemas próprios que executem esta função.

A componente de Gestão de Configuração é também parcialmente implementada, disponibilizando algumas funcionalidades como a activação ou desactivação de interfaces de rede.

A Gestão de Segurança é implementada, no próprio *OpenNMS*, através da gestão de acessos, seja localmente ou recorrendo a um servidor LDAP. Sendo também implementa através da integração com sistemas de detecção de intrusão (IDS) ou de vulnerabilidade, como o *Snort* ou o *Nessus*.

5.2.2. PREPARAÇÃO / INSTALAÇÃO

Para se proceder à instalação do *OpenNMS* são necessários os seguintes pré requisitos:

- Servidor *Linux*;
- *PostgreSQL*;
- *Java*;
- *JICMP*.

O projecto de monitorização tem como sistema operativo de suporte o *Ubuntu Server* versão 7.10 [24]. Baseado na distribuição *Debian*, este sistema oferece garantias de performance e robustez necessárias para o projecto que pretendemos alcançar.
A versão *Server* do *Ubuntu* está a entrar no mercado de servidores, oferendo o melhor software livre, numa versão estável, 100% suportada e sobre uma plataforma segura.
Desde o seu aparecimento o *Ubuntu* tem ganho quota de mercado nas organizações de todo o mundo dada a sua segurança e custo, mostrando ser eficiente energeticamente, e com poucas exigências a nível de hardware, quer relativamente à memória, quer ao espaço em disco necessários [25].
Depois de estabilizado o sistema operativo, foram instalados todos os pré-requisitos necessários:

- *PostgreSQL* (v8.2.11), *Java* (v5), *JICMP* (v1.0.8).

De seguida procedeu-se à instalação do *OpenNMS*, versão 1.6.4, seguindo o manual oficial [26]. Uma vez executados todos os *scripts* deu-se por terminada a instalação da aplicação e passando-se à fase de configuração.

5.2.3. CONFIGURAÇÃO

Para aceder ao sistema, acabado de instalar, direccionamos o browser para o URL http://ip.servidor:8980/opennms/. Sendo necessário efectuar autenticação para começar a interagir com a plataforma, Figura 5.1.
Os utilizadores da aplicação *OpenNMS* podem estar agrupados em grupos de utilizadores distintos. Os privilégios de acesso são definidos através destes grupos de utilizadores e podem comportar a diferenciação entre apenas leitura ou alteração de parâmetros, bem como, as categorias de informação ou mesmo os nós a que se tem acesso.
Um sistema *OpenNMS* suporta autenticação através do serviço LDAP, recorrendo ao módulo *OpenNMS User Synchronization*.

Por defeito, a plataforma está configurada para obtermos de imediato um resumo dos sistemas monitorizados, assim como, a possibilidade de aceder a dados detalhados ou ao menu de configurações.

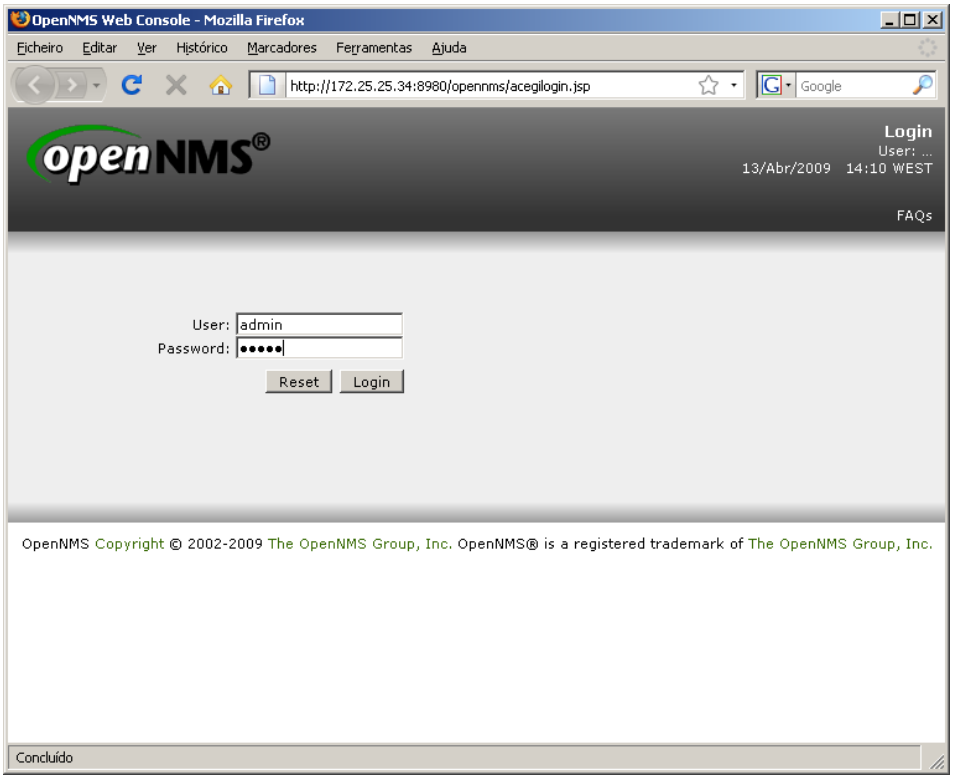

Figura 5.1 - OpenNMS – Login

A interface Web é método mais prático para a interacção com o *OpenNMS* nas tarefas do dia-a-dia. A primeira página transmite a informação geral sobre o estado da rede, agrupada por categorias que podem ser definidas pelos utilizadores. Esta informação disponibilizada é o número de alertas e a percentagem de disponibilidade, relativa aos nós incluídos na categoria.
Os nomes das categorias são *links*, para facilmente se aceder aos detalhes das informações constantes no sistema *OpenNMS*.
Além da informação sobre o estado geral do sistema monitorizado, é possível verificar Eventos, Alarmes e Notificações, e realizar a aceitação dos mesmos, bem como aceder directamente aos gráficos de desempenho disponibilizados e desenvolver novos.

5.2.4. CONFIGURAÇÃO AUTO DISCOVER

Esta funcionalidade de configuração permite definir quais são os sistemas a serem monitorizados. Esta possibilidade é interessante, uma vez que, podemos não querer monitorizar todo o parque informático ou todos os activos de rede. Esta definição pode ser feita de várias formas, das quais destacamos a possibilidade de se definir a gama de endereços IP que pretendemos monitorizar, Figura 5.2.

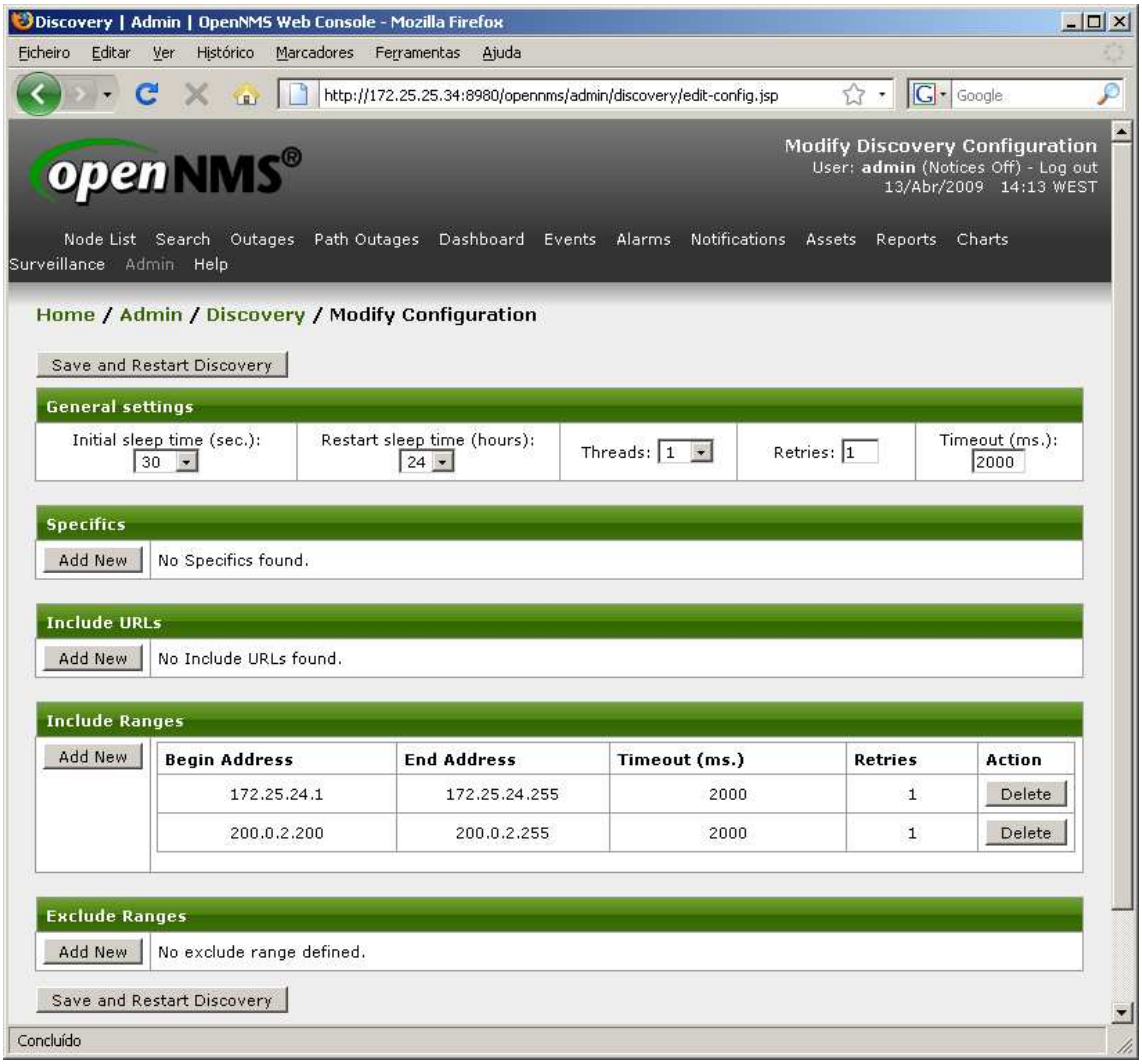

Figura 5.2 - OpenNMS - Config Auto Discovery

Podendo também ser configurado através de endereços IP únicos, gamas de endereços excluídos, ou através da utilização de um ficheiro que contenha a lista de todos os endereços pretendidos.

As configurações de endereços geradas através da interface Web ficam gravadas num ficheiro ilustrado na figura seguinte, Figura 5.3.

```
<?xml version="1.0" encoding="UTF-8"?>
<discovery-configuration
xmlns="http://xmlns.opennms.org/xsd/config/discovery" threads="1"
packets-per-second="1" initial-sleep-time="30000"
restart-sleep-time="86400000" retries="1" timeout="2000">
<specific retries="1" timeout="2000">172.25.255.253</specific>
<specific retries="1" timeout="2000">172.25.247.253</specific>
<specific retries="1" timeout="2000">172.25.239.253</specific>
<specific retries="1" timeout="2000">172.25.231.253</specific>
<specific retries="1" timeout="2000">172.25.223.253</specific>
<specific retries="1" timeout="2000">10.14.200.253</specific>
<include-range retries="1" timeout="2000">
<begin xmlns="">172.25.24.1</begin>
<end xmlns="">172.25.24.255</end>
</include-range>
<include-range retries="1" timeout="2000">
<begin xmlns="">200.0.2.200</begin>
<end xmlns="">200.0.2.255</end>
</include-range>
<include-range retries="1" timeout="2000">
<begin xmlns="">172.25.29.1</begin>
<end xmlns="">172.25.31.255</end>
</include-range>
</discovery-configuration>
```

Figura 5.3 - Ficheiro discovery-configuration.xml

5.2.5. MONITORIZAÇÃO SNMP

A monitorização de activos através de SNMP é uma mais-valia, uma vez que, através deste protocolo é possível recolher variáveis específicas dos equipamentos, sendo estas informações extremamente úteis para a correcta percepção da realidade dos sistemas que constituem o parque informático.

Para se efectuar monitorização através do protocolo SNMP é necessário configurar a gama de endereços (desde o endereço X até ao endereço Y) dos activos que pretendemos que sejam monitorizados via SNMP, bem como identificar os nomes das comunidades SNMP em que estes se inserem, Figura 5.4.

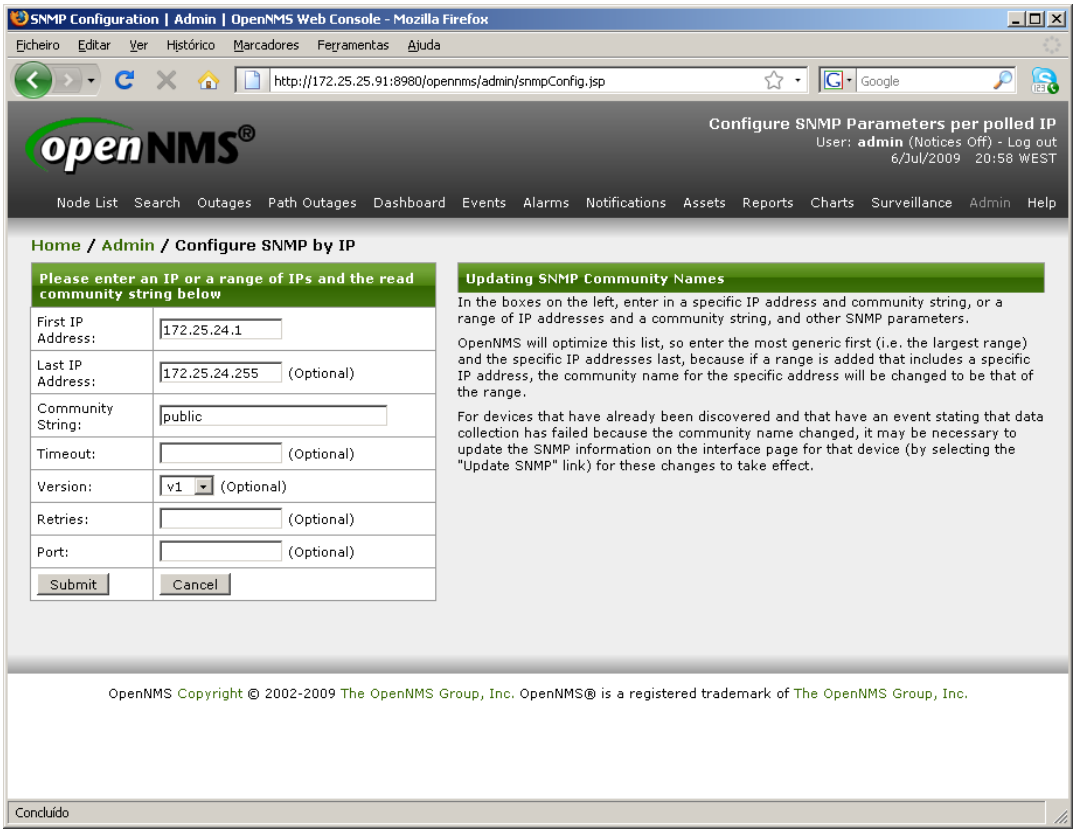

Figura 5.4 - OpenNMS - Configuração SNMP

Estes parâmetros ficam guardados no ficheiro ilustrado na figura seguinte, Figura 5.5.

```
<?xml version="1.0" encoding="UTF-8"?>
<snmp-config xmlns="http://xmlns.opennms.org/xsd/config/snmp"
port="161"
    retry="3" timeout="800" read-community="public" version="v1"
max-vars-per-pdu="10">
    <definition read-community="public" version="v1">
        <specific xmlns="">200.0.2.240</specific>
    </definition>
</snmp-config>
```

Figura 5.5 - Ficheiro snmp-config.xml

Embora o *OpenNMS* possa funcionar como ferramenta de gestão/monitorização de serviços, de disponibilidade ou de eventos sem recorrer ao SNMP, o uso deste protocolo acrescenta muitas funcionalidades e informações importantes à ferramenta.

No *OpenNMS*, o processo de *auto-discover* inicia-se através do envio de um *ping* para todos os endereços IP definidos. De seguida, caso exista uma resposta por parte do sistema destino é gerado um novo evento. Este evento chama o processo *capsd* que é responsável por verificar a disponibilidade dos serviços configurados no ficheiro ilustrado na figura seguinte, Figura 5.6.

```
<?xml version="1.0"?> <!-- 24 hours -->
<capsd-configuration
        rescan-frequency="86400000"
        initial-sleep-time="30000"
        max-suspect-thread-pool-size="6"
        max-rescan-thread-pool-size="3">
    <protocol-plugin protocol="ICMP" class-
name="org.opennms.netmgt.capsd.plugins.IcmpPlugin" scan="on">
        <property key="timeout" value="2000" />
        <property key="retry" value="1" />
    </protocol-plugin>
    <protocol-plugin protocol="HTTP" class-
name="org.opennms.netmgt.capsd.plugins.HttpPlugin" scan="on">
        <property key="port" value="80" />
        <property key="timeout" value="3000" />
        <property key="retry" value="1" />
    </protocol-plugin>
    <protocol-plugin protocol="FTP" class-
name="org.opennms.netmgt.capsd.plugins.FtpPlugin" scan="on">
        <property key="port" value="21" />
        <property key="timeout" value="2000" />
        <property key="retry" value="1" />
    </protocol-plugin>
    <protocol-plugin protocol="DNS" class-
name="org.opennms.netmgt.capsd.plugins.DnsPlugin" scan="on">
        <property key="port" value="53" />
        <property key="timeout" value="5000" />
        <property key="retry" value="1" />
        <property key="lookup" value="localhost" />
    </protocol-plugin>
    <protocol-plugin protocol="DHCP" class-
name="org.opennms.netmgt.capsd.plugins.DhcpPlugin" scan="on">
        <property key="timeout" value="3000" />
        <property key="retry" value="1" />
    </protocol-plugin>
    <protocol-plugin protocol="POP3" class-
name="org.opennms.netmgt.capsd.plugins.Pop3Plugin" scan="on">
        <property key="port" value="110" />
        <property key="timeout" value="3000" />
        <property key="retry" value="1" />
    </protocol-plugin>
</capsd-configuration>
```

Figura 5.6 - Ficheiro capsd-configuration.xml

Quando o SNMP está activo, o serviço *capsd* tenta receber informações do objecto *sysObjectID* através do nome da comunidade SNMP e número de porto, definidos no ficheiro *snmp-config.xml* (ou através do menu *Admin* – "*Configure SNMP by IP*").

Em caso de sucesso é assinalado o dispositivo de rede com SNMP activo e são realizados novos testes através do serviço *capsd*.

O processo de recolha de informação inicia-se pelos ramos *ipAddrTable* e *ifTable* do SNMP. Caso não seja possível, recolher esta informação, o processo de recolha termina, embora a informação previamente adquirida fique disponível.

De seguida são recolhidos dados referentes a cada endereço IP e a cada interface do dispositivo.

Exemplos de informação SNMP recolhida automaticamente pelo *OpenNMS* são ilustrados na figura seguinte, Figura 5.7.

SNMP Attributes	
Name	iR2230 KJD04881
Object ID	.1.3.6.1.4.1.1602.4.7
Location	MANUTENCAO 1 PISO
Contact	
Description	Canon iR2230 /P

SNMP Attributes	
Name	switch-infor
Object ID	.1.3.6.1.4.1.9.1.615
Location	A035
Contact	informatica.porto@rtp.pt
Description	Cisco IOS Software, C3560 Software (C3560-IPBASE-M), Version 12.2(25)SEE2, RELEASE SOFTWARE (fc1)..Copyright (c) 1986-2006 by Cisco Systems, Inc...Compiled Fri 28-Jul-06 07:19 by yenanh

SNMP Attributes	
Name	Manuten��o
Object ID	.1.3.6.1.4.1.848.10.37.4
Location	Un.Energia
Contact	informatica.porto@rtp.pt
Description	D-Link 802.11g AP

Figura 5.7 - Exemplos informação SNMP

5.2.6. ALERTAS POR EVENTOS

Uma das maiores vantagens de um sistema de auxílio à administração de sistemas é a possibilidade de enviar, de forma automática, mensagens de aviso sempre que algo de anormal ocorre [27].

A definição de “anormal” é feita pelo administrador, que define parâmetros que devem ser monitorizados e que despoletam alertas.

Esta Funcionalidade obriga a ser feita uma configuração prévia:

1) Configurar o *OpenNMS* para o envio de mensagens de correio electrónico;

2) Configurar destinos dos alertas;

3) Configurar os eventos que devem activar alertas.

Para **configurar o *OpenNMS* para enviar *e-mail* (1)**, é necessário aceder e editar o ficheiro ilustrado na figura seguinte, Figura 5.8.

```
org.opennms.core.utils.mailHost=172.20.40.14
org.opennms.core.utils.mailer=smtpsend
org.opennms.core.utils.transport=smtp
org.opennms.core.utils.debug=true
org.opennms.core.utils.smtpport=25
org.opennms.core.utils.smtpssl.enable=true

org.opennms.core.utils.useJMTA=false

org.opennms.core.utils.authenticate=true
org.opennms.core.utils.authenticateUser="email@rtp.pt"
org.opennms.core.utils.authenticatePassword="password"
```

Figura 5.8 - Ficheiro javamail-configuration.properties

As configurações deste ficheiro são elementares e referem-se apenas às definições necessárias para aceder ao servidor de correio electrónico. Os parâmetros que são necessários editar são: *mailHost* e *autenticate*, *autenticateUser* e *autenticatePassword* se o servidor de *e-mail* exigir autenticação.

A **configuração dos destinatários de alertas (2)**, são realizadas através da interface gráfica, na opção *Home* / *Admin* / *Configure Notifications* / *Destination Paths* / *Choose Targets,* Figura 5.9.

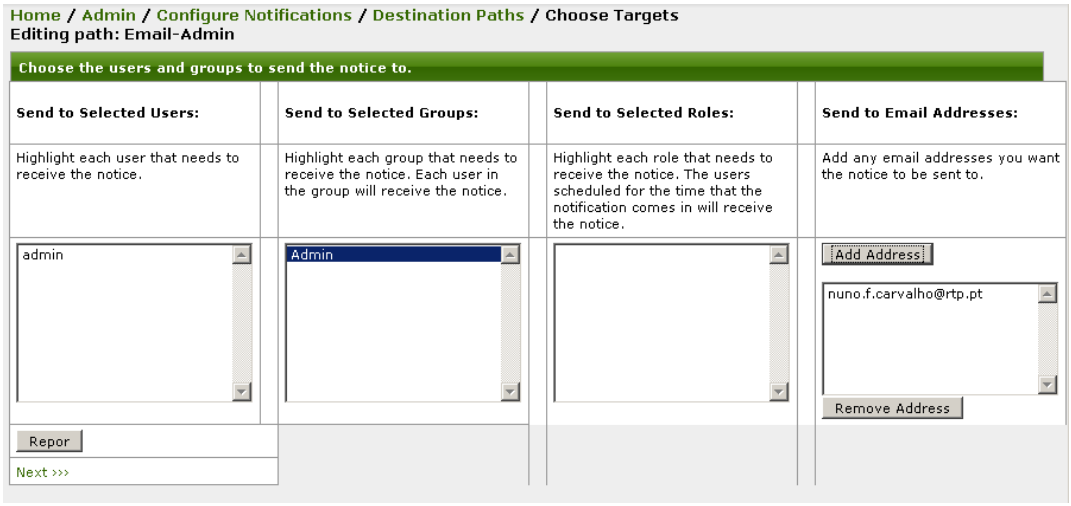

Figura 5.9 - Configuração destinatários alertas

As configurações realizadas, neste passo, ficam guardadas no ficheiro ilustrado na **Erro! A origem da referência não foi encontrada.**.

```
<?xml version="1.0" encoding="UTF-8"?>
<destinationPaths
xmlns="http://xmlns.opennms.org/xsd/destinationPaths">
  <ns1:header xmlns:ns1="http://xmlns.opennms.org/xsd/types">
    <rev xmlns="">1.2</rev>
    <created xmlns="">April 10, 2009 2:04:30 PM GMT</created>
   <mstation xmlns="">localhost</mstation>
   </ns1:header>
   <path name="Email-Admin" initial-delay="0s">
       <target interval="0m">
           <name xmlns="">Admin</name>
           <autoNotify xmlns="">on</autoNotify>
           <command xmlns="">javaEmail</command>
       </target>
       <target interval="0s">
           <name xmlns="">nuno.f.carvalho@rtp.pt</name>
           <autoNotify xmlns="">on</autoNotify>
           <command xmlns="">email</command>
       </target>
   </path>
</destinationPaths>
```

Figura 5.10 - Ficheiro destinationPaths.xml

Por último, falta a definição dos eventos que irão despoletar os alertas. A alterações de valores, que fazem **ocorrer o envio de um alerta (3)**, podem ser definidos via interface Web, em *Home / Admin / Configure Notifications / Event Notifications.*

O primeiro passo para a criação de um novo alerta é a escolha do evento que ao acontecer deverá accionar um alarme. Já existem inúmeros parâmetros que podem ser verificados constantemente pelo sistema, e muitos outros podem ser adicionados especificamente para a rede que estamos a verificar. Por omissão, no *OpenNMS*, não existem alertas previamente configurados e activos.

Na Figura 5.11 são ilustradas algumas das escolhas possíveis.

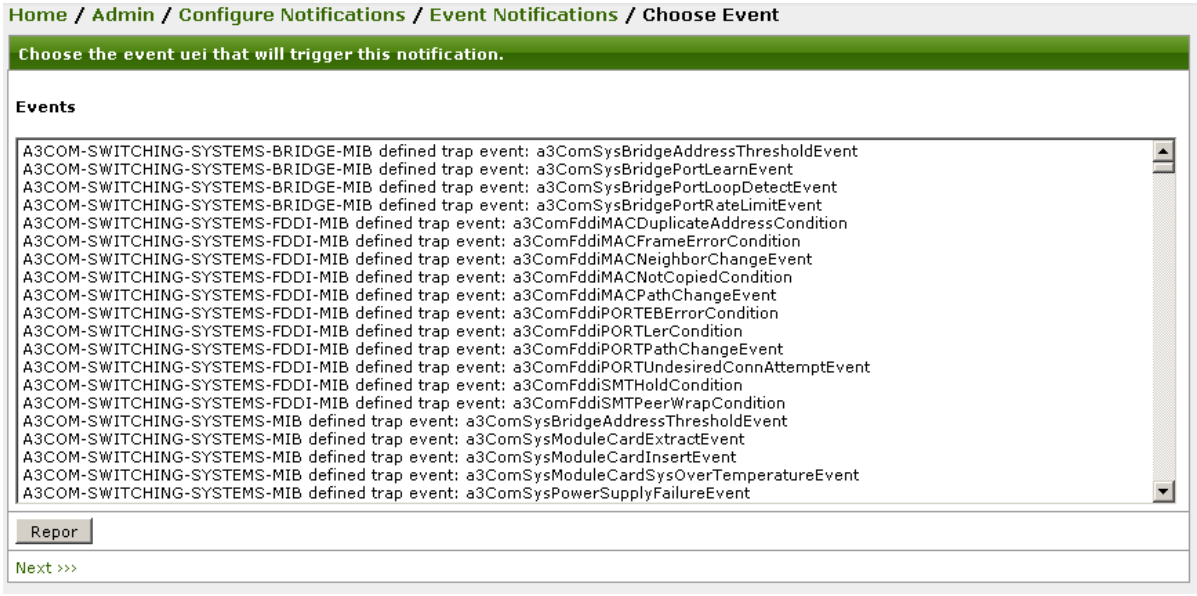

Figura 5.11 - Criação Alerta: Escolha evento

As possibilidades são muito abrangentes, contendo opções para muitos eventos internos, como por exemplo, detecção de activos, perda de comunicação com *hosts*, interfaces ou serviços, assim como eventos específicos para determinados fornecedores de equipamentos, como por exemplo, 3Com, Cisco, HP ou IBM. Um exemplo, de um evento existente por defeito é o "*OpenNMS-defined node event: interfaceDown*". Trata-se de um evento que é chamado sempre que internamente o *OpenNMS* detecta que um dos activos monitorizados ficou com uma interface em baixo.

Uma vez escolhido o evento pretendido, o passo seguinte é escolher a que activos este evento se refere. Este filtro pode ser aplicado a *hosts*, através do seu endereço IP, e/ou a serviços, Figura 5.12.

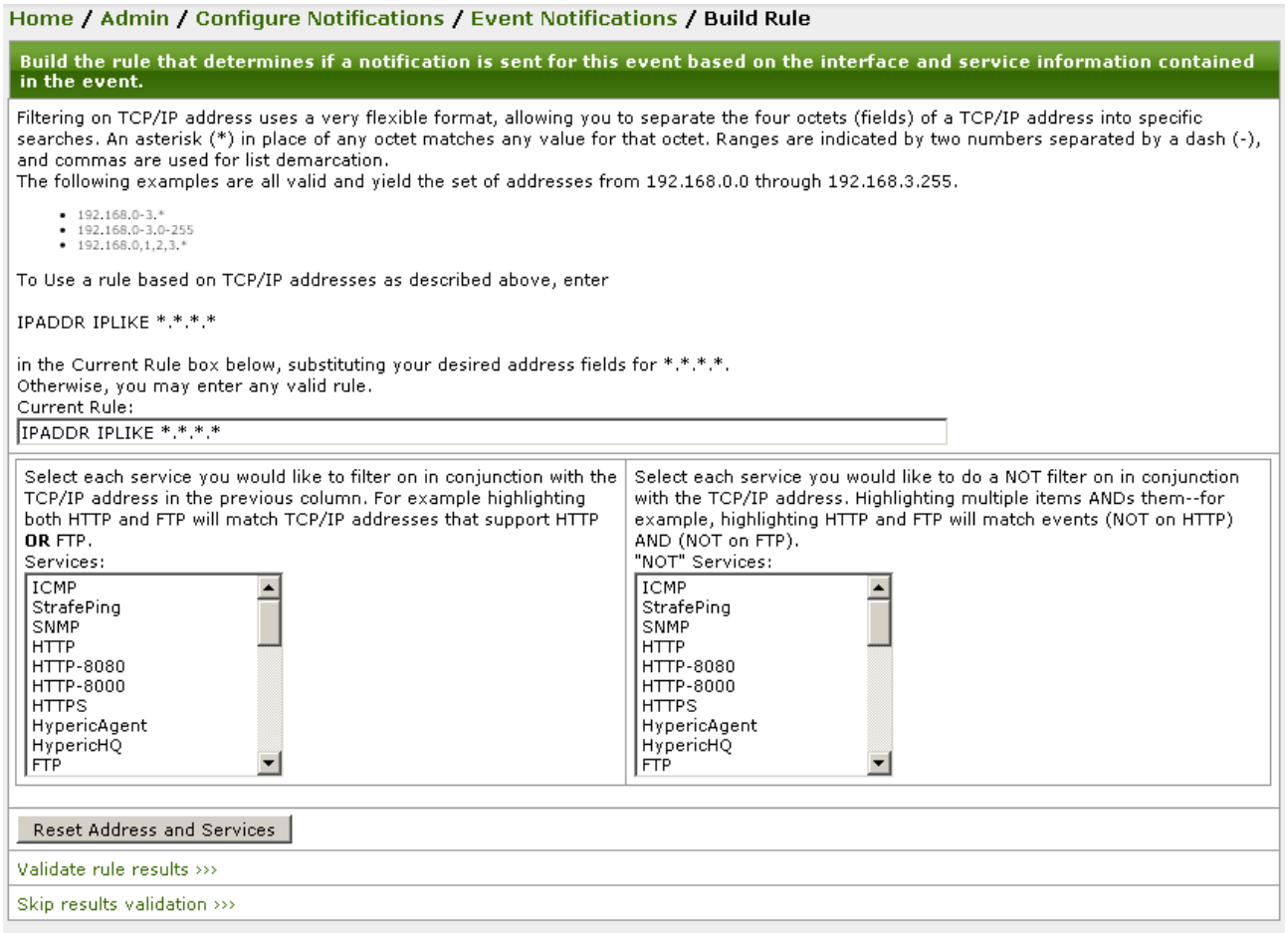

Figura 5.12 - Criação Alerta: Definição de Filtros

Um exemplo de aplicação deste alerta é definir que se destina apenas aos *switchs* da rede, utilizando o filtro por endereço IP, 192.168.89.100 -150.

Por fim, são também definidos os nomes e a respectiva descrição da regra, assim como o endereço de correio electrónico para o qual será enviado.

Paralelamente, existe também a possibilidade de personalizar o texto da mensagem, podendo ser composto por várias variáveis recolhidas pelo *OpenNMS*, tais como, a hora do evento, a importância do evento, o endereço IP, o nome do serviço, entre outros. A figura seguinte, Figura 5.13 ilustra esta possibilidade.

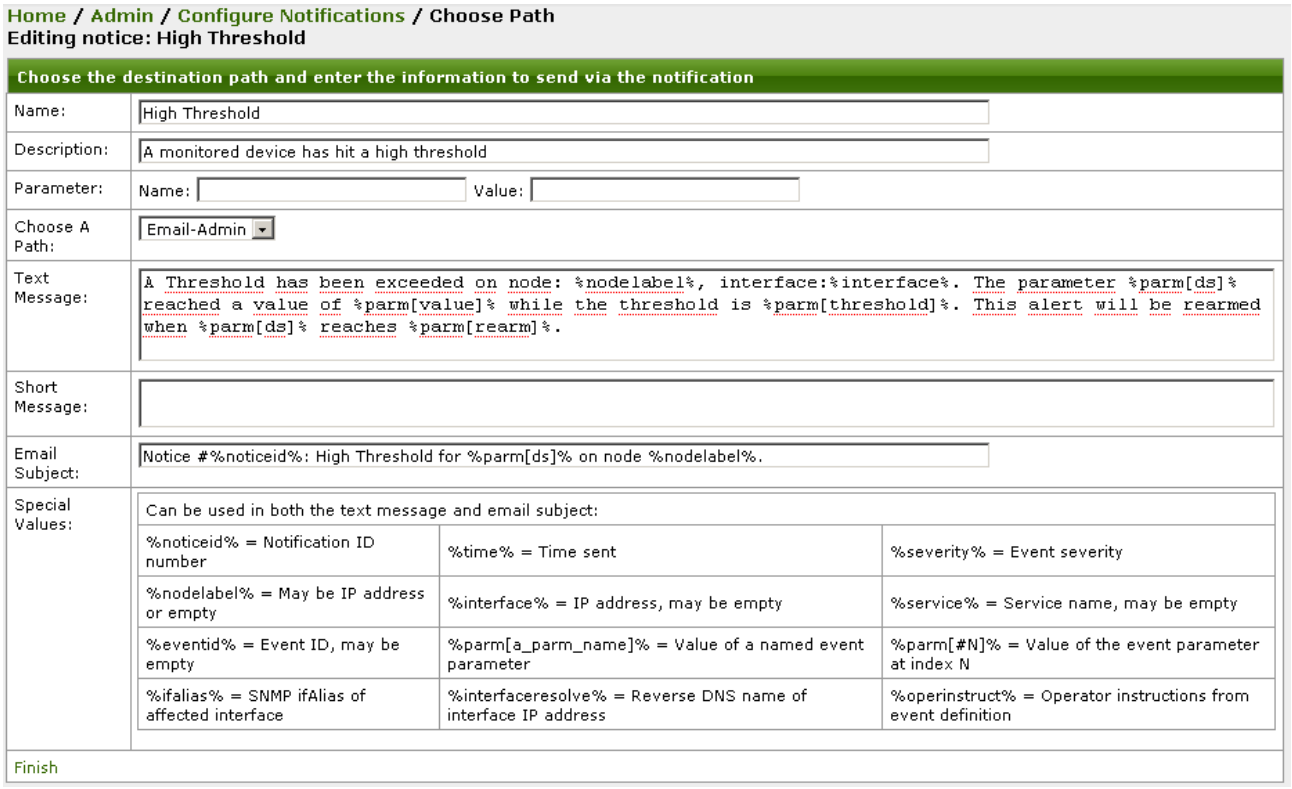

Figura 5.13 - Criação Alerta: Definição do mail

5.2.7. DEFINIÇÃO DE GRUPOS DE DISPOSITIVOS

O modo *Surveillance* [28], acessível na interface, permite que se agrupem os vários nós em grupos com significado para o utilizador, por exemplo áreas organizacionais, tipos de equipamento ou domínios.

No caso de uma organização grande, como o cenário em estudo, a RTP Porto, a subdivisão dos activos é vantajosa, de forma a organizar áreas distintas, que podem ser administradas por utilizadores diferentes.

Para se criar novos grupos de categorias deve-se aceder no menu de Administração à opção *Surveillance Categories*.

A figura seguinte, Figura 5.14, ilustra a interface que permite criar novas categorias, assim como associar dispositivos às categorias já criadas.

Para o cenário real, a RTP Porto, foram criadas as seguintes categorias:

- Biométrico;
- Impressoras;
- *Routers*;
- *Servers*;

- *Switches*.

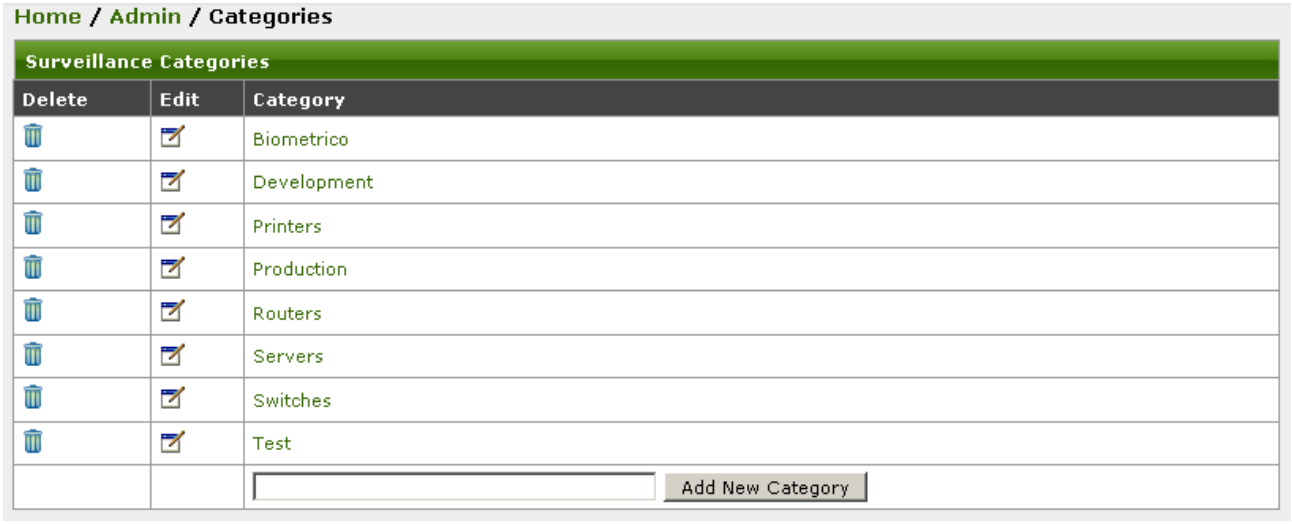

Figura 5.14 - Definição de grupos de dispositivos

5.2.8. DEFINIÇÃO DE TEMPOS DE MANUTENÇÃO

Durante o período de testes da aplicação *OpenNMS* surgiu uma tarefa de manutenção que iria obrigar ao corte do *link* entre o Porto e Lisboa, Figura 5.15. Uma vez que o sistema implementado estava a monitorizar activos de rede em Lisboa, com o corte do circuito de ligação obrigatoriamente estes activos monitorizados iria apresentar erros, durante o período de manutenção.

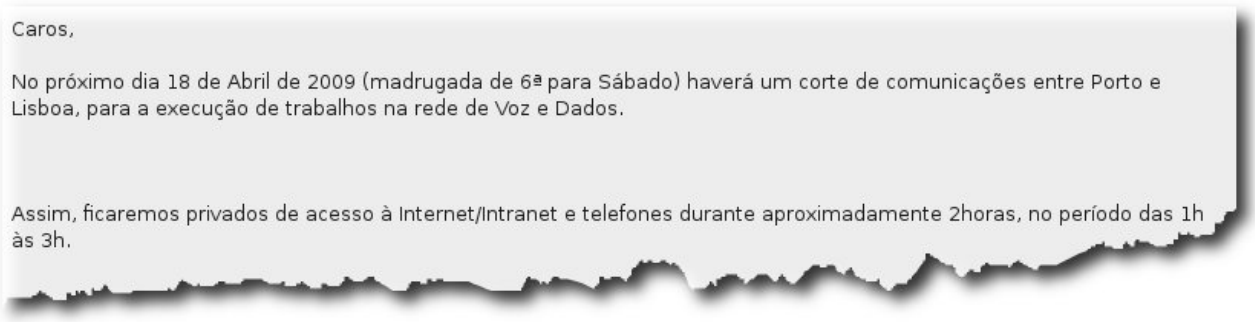

Figura 5.15 - Comunicado Interno

Assim, definiu-se no sistema um período de manutenção para que os erros detectados não fossem considerados. A definição de período de manutenção pode ser vista na figura seguinte, Figura 5.16.

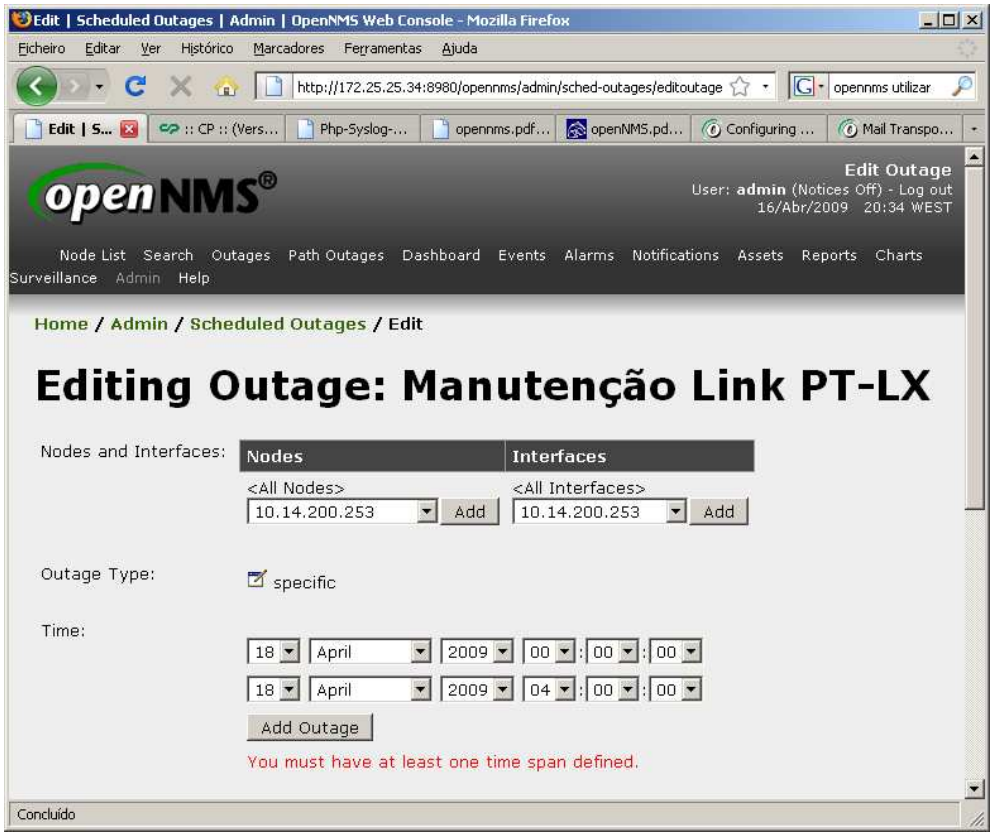

Figura 5.16 - Definição tempo de manutenção

5.2.9. RELATÓRIOS

A versão do *OpenNMS* instalada já contém um vasto reportório de relatórios disponíveis – Gráficos de disponibilidade, performance ou de recursos, bem como diversas estatísticas disponíveis no menu superior *Reports*.

São disponibilizados quatro grupos diferentes de relatórios.

- *Resource Graphs*;
- *KSC Performance, Nodes, Domain*;
- *Availability*;
- *Statistics Reports*.

Resource Graph, fornece uma forma fácil de visualizar alertas SNMP, tempos de resposta, bem como outras informações recolhidas através da rede sobre os nós monitorizados. Dependendo do activo em causa, e da informação que foi recolhida, várias informações estão disponíveis. Esta informação pode ser relativamente básica, como por exemplo, tempo de resposta ao

pedido ICMP, disponível na maioria dos activos, até informação mais complexa, como por exemplo, informação de tráfego, taxa de erros ou temperatura. Na realidade, o conhecimento que se pode obter está dependente do que é possível obter através de SNMP do dispositivo.

Os activos *Switchs* e *Routers* são os que mais informações disponibilizam, dado o seu funcionamento e capacidades. As informações mais úteis, para a correcta administração da rede da RTP Porto, prendem-se com o tráfego. É importante ter conhecimento sobre as ligações TCP/IP, eventuais erros, mensagens ICMP, Bits i*n/out*, pacotes perdidos ou descartados, etc.

No entanto, existem também outras informações que o *OpenNMS* pode recolher e que são úteis para a detecção de causas de problemas, tais como, temperatura do equipamento, utilização do UCP ou estado da memória, Figura 5.17.

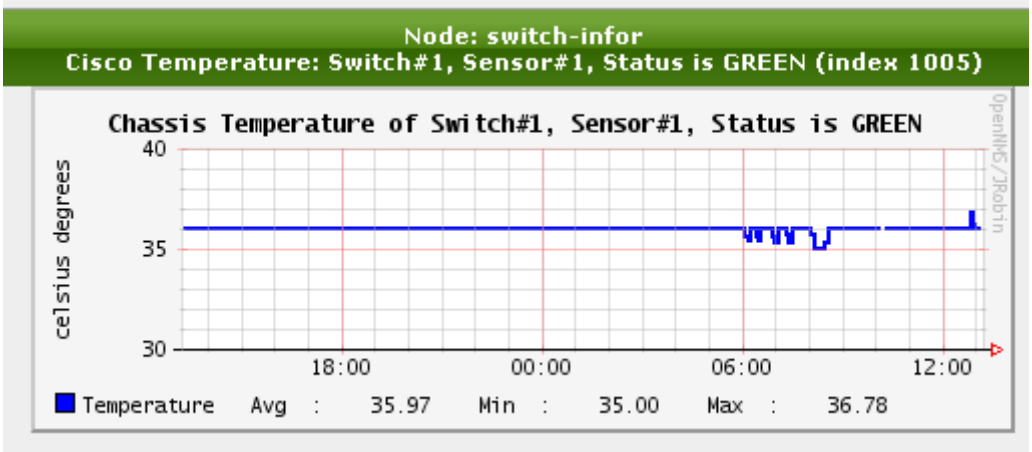

Figura 5.17 - Gráfico Temperatura Cisco

Outro tipo de dispositivo que, através do SNMP, consegue obter informação diversificada são as impressoras de rede, Figura 5.18. Pelo simples facto de se tratar de um dispositivo de rede já disponibiliza toda a informação relativa ao tráfego da mesma ou aos tempos de resposta. Paralelamente, é possível obter informação específica relativa às suas funcionalidades. Informações que podem ser úteis para a apoiar a interpretação da sua:

- Utilização da memória;
- Número de utilizadores;
- Disponibilidade do toner;
- Páginas impressas;
- Etc.

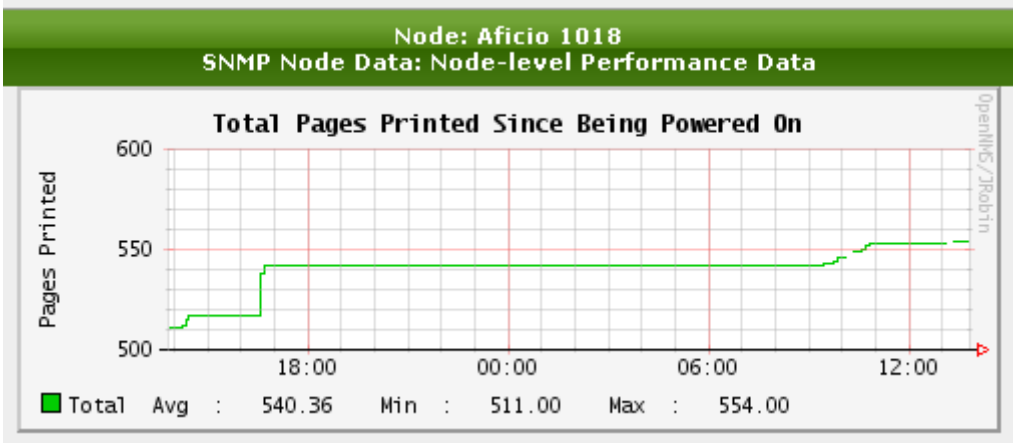

Figura 5.18 - Gráfico Páginas impressas

Outro tipo de relatório disponibilizado é o ***KSC (Key SNMP Customized) Performance Reports***, que permite ao administrador de sistema criar gráficos baseados em informações SNMP. Estes gráficos são muito flexíveis quer ao nível de dados, quer relativamente ao tipo de gráficos e período temporais que se podem incluir.

Após a personalização de um relatório, este pode ser guardado para uso futuro.

Um relatório por nó (*node*) mostra informação de todas as interfaces que disponibilizam SNMP.

Os relatórios de disponibilidade (*Availability)* fornecem informação gráfica ou numérica das métricas de nível de serviço por um período de tempo.

Os relatórios gerados, internamente, e posteriormente enviados por correio electrónico, podem ser no formato PDF ou HTML, e podem conter uma vista gráfica da disponibilidade para o período definido (mês actual, mês anterior ou últimos 12 meses), Figura 5.19.

Por último os relatórios estatísticos (*Statistics Reports*) disponibilizam informação sumária a partir das informações numéricas recolhidas (tempo de resposta, SNMP, performance, etc.). Além das informações *standard* recolhidas pelo sistema, muitas mais podem ser obtidas, através do uso e configuração da ferramenta RRDTOOL, que faz parte do *OpenNMS*.

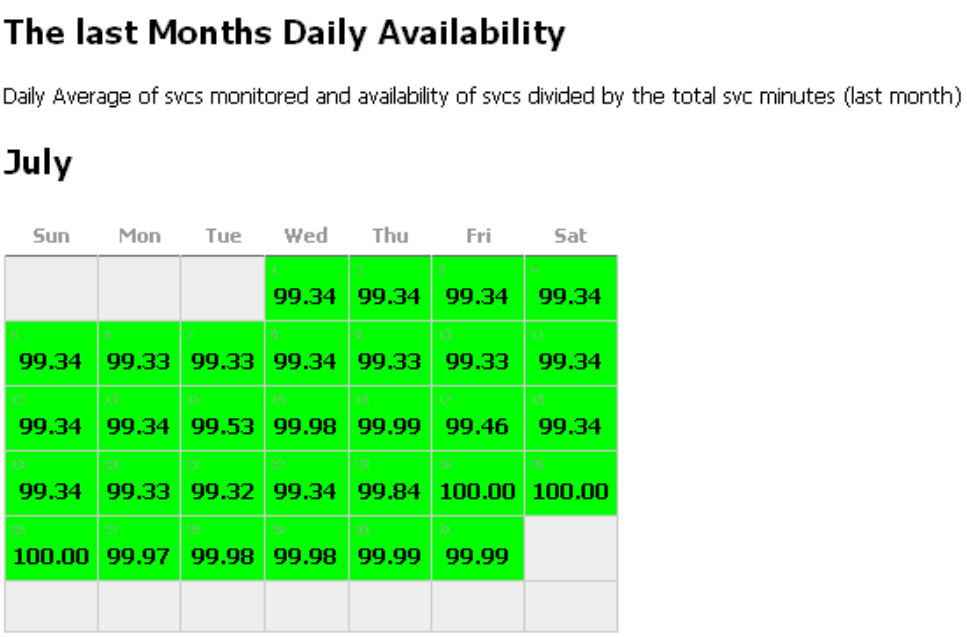

Figura 5.19 - Exemplo Relatório disponibilidade mês anterior

5.3. GESTÃO DE ACTUALIZAÇÕES

Durante o decorrer deste projecto, centrado no cenário da RTP Porto e delegações do norte do país, os serviços centrais da informática, sediados em Lisboa, também aplicavam esforços no sentido de encontrar uma solução de gestão para efectuar actualizações de uma forma centralizada em toda a empresa.

Com o intuito de procurar uma solução integrada, foi estudada a hipótese de configurar o *OpenNMS* para suportar a gestão de actualizações do parque informático. Várias alternativas foram exploradas, desde a integração de módulos específicos para esta área de gestão, até à interligação com outras aplicações que acrescentassem estas funcionalidades. Após ter sido efectuada uma pesquisa exaustiva, conclui-se ser impossível dotar a aplicação *OpenNMS* desta capacidade, gestão de actualizações.

Simultaneamente, a equipa de sistemas de Lisboa, procedeu à implementação de uma solução global de inventariação e gestão de actualizações do parque informático. Pelo que esta nova aplicação veio dar resposta a esta necessidade específica.

A opção tomada pelos serviços centrais foi o *Microsoft System Management Server* 2003 (SMS 2003). Esta opção veio trazer uma redução de custos de operação, optimização das tarefas de gestão e manutenção do parque informático e um controlo de inventário de hardware e software, em toda a empresa, incluindo os *sites* abrangidos por este projecto.

5.4. GESTÃO DE ACTIVOS DE REDE

A aplicação *OpenNMS* não tem capacidade para gerir activos de rede, apesar da monitorização exaustiva que faz a estes equipamentos.

O *OpenNMS* foi configurado para extrair o máximo de informação possível dos equipamentos de rede existentes.

Tendo sido possível verificar a sua aptidão para a monitorização de activos de rede, uma vez que efectua a recolha constante de informações que suportam essa análise: parâmetros como Utilização (interfaces, processador); Tráfego (Bytes *in/out*, tempo de resposta ao *ping*); Erros (falhas, descartes, perdas); etc.

Convém, também referir que esta capacidade aplica-se a activos Cisco e de outras marcas, como a IBM ou 3Com.

No entanto, em virtude de ser incapaz de realizar a gestão das configurações foi necessário manter a solução anterior – *Cisco Network Assistant* – como solução de gestão de activos.

Com a diferença de que se passou a ter o auxílio do *OpenNMS* na monitorização em tempo real, dos equipamentos e no envio de alertas no caso de serem detectadas irregularidades no seu funcionamento.

A monitorização realizada pela aplicação proprietária da Cisco, embora bastante completa, deixou de ser necessária ao ser convenientemente substituída pelo *OpenNMS*, remetendo-se apenas às funções de interface com os activos de rede para realização de configurações.

5.5. RESULTADOS

Com uma curva de aprendizagem algo lenta, em que muito contribui a complexidade das configurações, o *OpenNMS* mostra-se muito completo e flexível para monitorizar as necessidades de praticamente todos os administradores.

5.5.1. MONITORIZAÇÃO

Ao nível da monitorização, foram notórias as potencialidades disponibilizadas pelo *OpenNMS*, principalmente a nível de dados de tráfego, aumentando significativamente o número e diversidade dos dados recolhidos.

Relativamente às funcionalidades expectáveis, o *OpenNMS* mostrou ser um sistema capaz, que cumpre com qualidade a monitorização da rede e dos sistemas, fornecendo muitas informações úteis, tanto para a rápida actuação em caso de problemas como para uma análise intensa *à posteriori*, de forma a detectar e corrigir anomalias ou simplesmente a permitir implementar melhorias no parque informático e principalmente na rede de comunicações.

Se considerarmos o *OpenNMS* como uma ferramenta para monitorizar tudo, torna-se algo decepcionante. Isto deve-se ao facto de esta ferramenta possuir enormes capacidades para analisar a rede informática mas ser relativamente limitada quando a função é monitorizar computadores.

À medida que o processo foi sendo desenvolvido e foram sendo colmatadas as necessidades previamente impostas, novas limitações foram aparecendo, pois foram surgindo novas ideias de monitorização.

Da experiência adquirida, com a utilização do *OpenNMS*, dois factores destacaram-se como sendo desfavoráveis: a inexistência de um mapa da rede, ou seja, um mapa global e completo, ou mesmo um mapa dos equipamentos activos de rede (*switchs* e *routers*); e a falta de capacidade para extrair mais informações dos computadores (servidores ou não).
A disponibilidade de Informação detalhada sobre os sistemas operativos, o hardware ou das aplicações, é fundamental para o bom desempenho das tarefas de administrador de sistemas e responsável pelas TIs. Este ponto em concreto, foi colmatado com recurso à aplicação – Spiceworks – que se revelou ser superior para esta funcionalidade específica.

5.5.2. ALERTAS POR EVENTOS

O sistema de alertas implementado pelo *OpenNMS* é certamente um dos seus pontos fortes. Com enormes capacidades de análise sobre os dados recolhidos e de definição de filtros para permitir desencadear alertas. Convém, também salientar a existência da possibilidade de configurar várias alternativas para enviar os alertas, tais como, correio electrónico, mensagem de telemóvel ou mesmo contacto através de programas de conversação instantânea.
O facto de se saber que ao acontecer qualquer evento anormal serão enviados avisos, transmite segurança aos administradores do sistema, permitindo que estes não necessitem de estar a monitorizar o sistema de uma forma permanente.
Complementado com um registo exaustivo de todos os dados obtidos e de todos os eventos automaticamente detectados, esta ferramenta, fornece praticamente toda a informação necessária para se proceder à resolução de problemas e para efectuar análise do desempenho das tecnologias de informação envolvidas.
Nesta implementação consideraram-se os seguintes factores críticos para despoletar alertas:

- Servidores – falhas interfaces, falhas de serviços, não resposta dos servidores;
- Activos de Rede – interfaces críticas em baixo, não resposta dos activos, alterações de configuração;
- Rede – valores de tráfego elevado.

5.5.3. GESTÃO DE ACTUALIZAÇÕES

A gestão automática de actualizações é um passo importante para o funcionamento eficiente da equipa responsável pelo parque informático, uma vez que, se trata de uma tarefa morosa e maçadora que ocupa muito tempo de trabalho.
A solução – *OpenNMS* – escolhida e implementada não suporta a gestão de actualização, no entanto, e como já foi referido, foi implementada uma solução para tal – *Microsoft System Management Server* – central de distribuição automática de software, pelo que foi possível

completar a solução aqui proposta conseguindo criar-se uma plataforma de gestão capaz de cobrir também esta funcionalidade.

Esta aplicação permite aceder às últimas actualizações disponibilizadas, identificar máquinas desactualizadas ou vulneráveis e rapidamente instalar todos os *updates* necessários. A adopção da solução da *Microsoft* garantiu também uma qualidade de serviço mais elevada e a uniformização de todos os postos de trabalho, sem requer intervenções individuais e presencias de um técnico.

Com o decorrer do tempo alguns dos objectivos que se espera alcançar são:

- Transparência e normalização do sistema;
- Redução dos custos de *Helpdesk*;
- Operações normalizadas em todos os postos de trabalho;
- Acréscimo de segurança.

5.5.4. GESTÃO DE ACTIVOS DE REDE

Como referido no Capítulo 5.4 – Gestão de Activos de Rede, a aplicação previamente utilizada para gestão de activos, *Cisco Network Assistant*, é proprietária. Esta aplicação permite gerir a grande maioria dos activos de rede existentes. Por esta razão, seria difícil encontrar uma solução tão eficaz na gestão destes equipamentos. Pelo que, restava apenas efectuar a sua integração com a aplicação *OpenNMS*. No entanto, e apesar dos esforços despendidos, tal não foi possível.

Dadas as circunstâncias, optou-se por manter toda a monitorização, detecção de eventos e envio de alarmes centralizados na solução implementada, recorrendo à aplicação da Cisco, apenas quando necessário reconfigurar os equipamentos ou efectuar cópias de segurança das configurações.

6. CONCLUSÕES

6.1. INTRODUÇÃO

Neste capítulo sintetiza-se o trabalho desenvolvido avaliando-se as respectivas contribuições, apresentam-se as conclusões, e apontam-se sugestões para trabalho futuro.

6.2. SÍNTESE

A massificação da utilização das tecnologias de informação e da Internet para os mais variados fins, e nas mais diversas áreas, levantou problemas de gestão das infra-estruturas de informática, ímpares até ao momento. Paralelamente, o aumento do grau de complexidade das redes e do seu tamanho exige o emprego de um sistema de gestão que proporcione qualidade de serviço, proactividade, diferenciação de tráfego e o suporte multifacetado de serviços, assim como integração com o processo de serviços e negócio.

O presente trabalho restringiu-se apenas ao estudo de mecanismos e soluções de gestão de redes e sistemas para o caso particular da RTP Porto, deixando ficar de fora muitas outras áreas também importantes para o bom funcionamento das infra-estruturas informáticas, tais como, a área do armazenamento de dados e a área da segurança.

Este trabalho fez uma análise dos requisitos necessários contemplar no caso particular em estudo; estudou um conjunto de soluções existentes no mercado para identificar as soluções mais adequadas; propôs uma solução e procedeu à sua implementação e efectuou uma série de análises para validar a solução proposta.

6.3. CONCLUSÕES

Ao longo do desenvolvimento do trabalho são várias as conclusões que se podem retirar. No entanto, é de referir que uma gestão efectiva não depende apenas do estudo efectuado e da implementação da melhor solução encontrada, mas também, da existência de um conhecimento profundo, quer das tecnologias envolvidas, quer da organização física e lógica da infra-estrutura. Como tal, é de referir que muito trabalho de análise e exploração, de diversas situações que ocorrem durante o normal funcionamento da infra-estrutura em estudo, não é passível de ser enumerado mas que constitui o contributo essencial para se obter o conhecimento e sensibilidade necessárias para implementar um conjunto de soluções e práticas para uma gestão efectiva.

A implementação, numa fase inicial, foi apoiada pela muita e boa documentação existente *online*, ainda que muitas vezes apenas se refira à configuração através de ficheiros, descurando a vertente gráfica, que permite as mesmas parametrizações mas de uma forma mais cómoda e visualmente mais atractiva.

O *OpenNMS* é um produto, que apesar de distribuído gratuitamente, possui uma vasta equipa a desenvolve-lo desde o ano 2000, o que o torna um produto “maduro” e completo.
Apesar de o sistema ter sido desenvolvido e trabalhado, em cima de uma imagem virtual, que tem logo à partida desvantagens ao nível do desempenho, o sistema permaneceu estável durante os meses em que decorreu o projecto, apenas sofrendo algumas interrupções resultantes da falta de rede, e reinícios forçados da máquina física que suportava a máquina virtual.

Dos resultados apresentados, podem-se tirar algumas conclusões:

- *OpenNMS* é uma plataforma robusta e flexível;
- É um projecto *Open Source*, com muita informação disponível *online*;
- A instalação e configurações iniciais são tarefas relativamente complexas;
- A existência de uma interface gráfica permite, no entanto, facilitar a tarefa de configuração;
- A ausência de um mapa de rede é uma desvantagem;
- A informação recolhida através de monitorização, relativamente aos postos de trabalho, é pouco detalhada;
- Falta integrar no projecto ferramentas de gestão e de distribuição de software e controlo de licenças.

6.4. TRABALHO FUTURO

Neste trabalho propôs-se um modelo de gestão, e aplicou-se o modelo a um cenário prático. Tanto no modelo de gestão, como na sua aplicação prática, ficaram alguns problemas por resolver que se apresentam nesta secção. Primeiro apresentam-se sugestões para melhorias no modelo de gestão e por fim identificam-se possíveis direcções para trabalho futuro, que correspondem a evoluções do modelo de gestão proposto,

6.4.1. MELHORAMENTOS NA APLICAÇÃO PRÁTICA DO MODELO

O modelo prático implementado mostrou-se eficaz nas tarefas para as quais foi configurado. Nomeadamente, recolha automática de informação diversa e que permite apoiar o desempenho das tarefas do administrador de sistemas, no entanto esta informação podia ter sido utilizada para efectuar diversas análises que poderiam vir a permitir melhorar o desempenho de toda a infra-estrutura.

Ficaram, também por implementar funcionalidades como a execução automática de comandos despoletados por eventos, que podem contribuir para uma resolução mais rápida e automática de problemas.

Outra característica útil do *OpenNMS* é transformá-lo no receptor dos alertas SNMP (SNMP *traps*) de todos os equipamentos, bastando para isso, configurar cada um deles com o destino para onde devem ser enviados os avisos gerados internamente.

Embora o sistema *OpenNMS* possa ser executado em computadores mais obsoletos ou mesmo numa máquina virtual, quanto maior for a capacidade de processamento e a largura de banda disponível para a realização da monitorização, melhores e mais rápidos serão os resultados.

Melhorando estes dois parâmetros da máquina (processador e largura banda) é possível diminuir o período das verificações dos sistemas monitorizados, aumentando a fiabilidade dos resultados apresentados.

Não sendo o OpenNMS uma solução que responde a todas as necessidades assinaladas e não sendo possível interligar a solução implementada com os outros dois sistemas existentes – *Cisco Network Assistant* e *SpiceWorks* – manter os três em paralelo revelou-se uma solução quase perfeita. Apesar do acréscimo de trabalho, no que se refere a configuração e manutenção dos três sistemas, é possível extrair do conjunto das aplicações toda a informação necessária para obter uma visão global, prática e imediata das Tecnologias de Informação envolvidas na RTP Porto. Optou-se por retirar o melhor da solução implementada, o *OpenNMS*, delegando para as outras duas aplicações apenas as funções que esta aplicação não é capaz de executar.

6.4.1. ÁREAS DE INVESTIGAÇÃO FUTURA

A implementação deste projecto, além de mostrar as enormes necessidades de monitorização existentes nestes ambientes também permitiu demonstrar que existem outros aspectos que devem ser tidos em conta na escolha de uma solução integrada.

Paralelamente, permitiu compreender que será difícil encontrar uma solução que possa satisfazer de uma forma permanente todos os requisitos e as necessidades. Trata-se de um ambiente onde está patente uma constante evolução tecnológica, sendo portanto necessário encontrar soluções que garantam a possibilidade de continuar a gerir de uma forma integrada. No entanto, esta tarefa deve ser realizada com a consciência de que novas necessidades de gestão vão surgir para as quais se espera ser possível encontrar soluções e as integrar na nossa plataforma de gestão.

Convém, também destacar, que para além das áreas investigadas neste projecto, gestão de redes e de sistemas, muitas outras devem ser também objecto de estudo e devem fazer parte de um sistema de gestão integrado. Das quais se destacam a gestão de armazenamento, política de *backups* ou a segurança.

1. ACRÓNIMOS

ACK - Acknowledgment

API – Application Programmable Interface

ARPA – Advanced Research Projects Agency

ASN.1 – Abstract Syntax Notation version 1

ATM – Asynchronous Transfer Mode

B-ISDN – Broadband Integrated Services Digital Network

BML – Business Management Layer

CI – Component Interface

CIM – Common Interface Model

CMIP – Common Management Information Protocol

CMISE – Common Management Information Service

CMOT – CMIP Over IP

CNA - Cisco Network Manager

DHCP – Dynamic Host Configuration Protocol

DMI – Desktop Management Interface

DMTF – Desktop Management Task Force

DNS – Domain Name Server

DoD – Department of Defence

EML – Element Management Layer

GSM – Global System for Mobile communications

HTTP – HyperText Transfer Protocol

IAB – Internet Architecture Board

ICMP – Internet Control Message Protocol

IP – Internet Protocol

IPX – Internetwork Packet Exchange

ISDN – Integrated Services Digital Network

ISO – International Organization for Standardization

ITU-T – International Telecomunications Union - Telecommunication Standardization Sector

JMX – Java Management eXtensions

LDAP – Lightweight Directory Access Protocol

MI – Management Interface

MIB – Management Information Base

MIF – Management Information Format

NML – Network Management Layer

OSI – Open System Interconnection

PDU – Protocol Data Unit

RFC – Request for Comments

RMON – Remote Monitoring

SI – Sistema de Informação

SMI – Structure of Management Information

SML – Service Management Layer

SMTP – Send Mail Transfer Protocol

SNMP – Simple Network Management Protocol

TCP – Transmission Control Protocol

TI – Tecnologias de Informação

TMN – Telecommunication Management Network

VLAN – Virtual Local Area Network

VOIP – Voice Over IP

WBEM – Web Based Enterprise Management

2. REFERÊNCIAS

[1] Estudo do Protocolo SNMP
http://www.filipefreitas.net/papers/filipefreitas_net_estudo_snmp.pdf

[2] SNMP: Birth and Evolution
http://www.et.put.poznan.pl/snmp/intro/ihistor2.html

[3] RFC1052 IAB Recommendations for the Development of Internet Network Management Standards

[4] RFC1155 Structure and Identification of Management Information for TCP/IP-based Internets

[5] ISO8824 Abstract Syntax Notation One (ASN.1): Specification of basic notation

[6] RFC1905 Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)

[7] RFC1906 Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)

[8] RFC1909 An Administrative Infrastructure for SNMPv2

[9] RFC1910 User-based Security Model for SNMPv2

[10] RFC2271 An Architecture for Describing SNMP Management Frameworks

[11] RFC3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

[12] Djamel Sadok, Dêmio Mariz, “Gerenciamento de Redes”, 2003
http://www.di.ufpe.br/~dmts/rmon/rmon.pdf

[13] Lisandro Granville, “Gerência e Aplicações de Rede”
http://www.inf.ufrgs.br/granville/Gerencia/Programa/Mod12/Mod12_1.pdf

[14] RFC1757 Remote Network Monitoring Management Information Base

[15] JMX
http://java.sun.com/javase/technologies/core/mntr-mgmt/javamanagement/

[16] OpenView
http://www.hp.com/openview

[17] NetView
http://www.ibm.com/software/tivoli/products/netview/

[18] IBM Tivoli NetView DataSheet
ftp://ftp.software.ibm.com/software/tivoli/datasheets/netview.pdf

[19] SCCM
http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx

[20] OpenNMS
http://www.opennms.com/
[21] Landesk
http://www.landesk.com/
[22] Spiceworks Desktop Overview
http://community.spiceworks.com/help/Spiceworks_Desktop_Overview
[23] Nuno Carvalho, “Organizações e Segurança Informática”, 2009
[24] Ubuntu
http://www.ubuntu.com/
[25] Ubuntu Server Edition
http://www.ubuntu.com/products/whatisubuntu/serveredition
[26] Manual Oficial de Instalação (Sistemas Operativos Debian)
http://www.opennms.org/index.php/Installation:Debian
[27] Configuring notifications (OpenNMS Wiki)
http://www.opennms.org/wiki/Configuring_notifications
[28] Neil H. Watson, “A Review of OpenNMS”
http://technocrat.watson-wilson.ca/blosxom/blosxom/computer/onmsreview.html