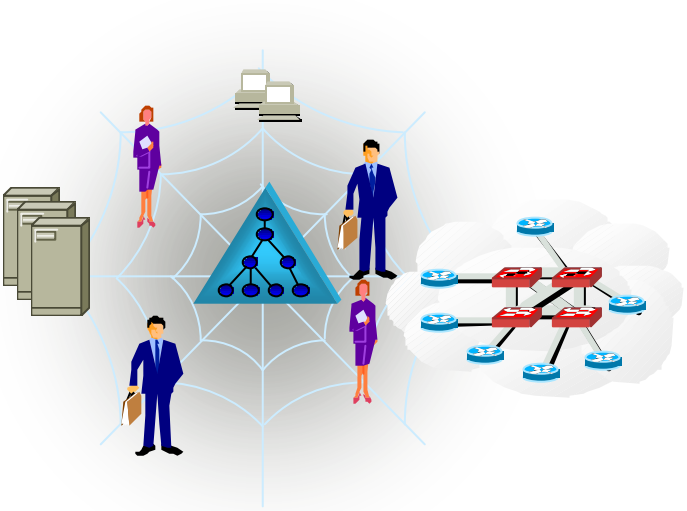
Universidade de Aveiro Departamento de Electrónica e Telecomunicações
2001

Ricardo Torres Martins

Arquitecturas e Ferramentas para Gestão de Redes e Sistemas – Um Caso de Estudo




Universidade de Aveiro Departamento de Electrónica e Telecomunicações
2001

Ricardo Torres Martins

Arquitecturas e Ferramentas para Gestão de Redes e Sistemas – Um Caso de Estudo

dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica do Dr. José Luís Guimarães Oliveira, Professor Associado do Departamento de Engenharia Electrónica e Telecomunicações da Universidade de Aveiro e do Dr. Joaquim Arnaldo Carvalho Martins, Professor Associado com Agregação do Departamento de Engenharia Electrónica e Telecomunicações da Universidade de Aveiro

o júri

presidente

Professor Doutor Joaquim Arnaldo Carvalho Martins
Professor Associado com Agregação da Universidade de Aveiro

Professor Doutor José Luís Guimarães Oliveira
Professor Associado da Universidade de Aveiro

Professor Doutor Alexandre Júlio Teixeira dos Santos
Professor Associado do Departamento de Informática da Escola de Engenharia da Universidade do Minho

agradecimentos

Gostava de aproveitar este espaço para agradecer a todos aqueles que, de alguma forma, contribuíram para o desenvolvimento deste trabalho e para a prossecução de uma experiência enriquecedora, assinalando as referências mais marcantes.

Ao Prof. Doutor José Luís Oliveira e Prof. Doutor Joaquim Arnaldo Martins, meus orientadores, por todo o apoio científico e pedagógico e pela palavras de encorajamento nos momentos em que foram mais necessárias.

À minha família agradeço o apoio sempre manifestado e que me fez chegar a este momento da minha vida.

À minha esposa, Élia Monteiro, pela sua permanente compreensão e motivação, em todos os momentos desta jornada.

Por último, agradeço a todos os meus amigos, que ficarão no anonimato, para não correr o risco de esquecer algum.

resumo

O trabalho desenvolvido teve por objectivos identificar e estudar as normas, mecanismos, políticas e aplicações a utilizar na gestão de uma infra-estrutura de informática, respondendo aos actuais requisitos das Instituições.

O "focus" da gestão têm-se vindo a alterar ao longo dos últimos anos, fruto de um contínuo acompanhamento da evolução das infra-estruturas de informática e dos serviços que elas suportam, o que implica um investimento constante, quer na actualização de meios tecnológicos, quer na actualização de conhecimentos dos recursos humanos.

Com a consciência 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, as directivas de aprendizagem seguidas ao longo da dissertação tiveram por base estes propósitos.

O estudo efectuado culminou com a implementação prática de sistema de gestão adequado a uma infra-estrutura de informática, bastante rica na diversidade de tecnologias e sistemas. Desta implementação serão apresentados alguns resultados que reiterarão a necessidade e vantagens de utilizar um sistema de gestão na infra-estrutura estudada.

abstract

The work developed had the objective of identifying and studying the standards, mechanisms, policies and applications to be used in the management of a computing substructure, answering the present requirements of the institutions.
The “Focus” of the management has come to change during the recent years, fruit of a continued accompanying of the evolution of substructures of computing and the services they support, which implicates a constant investment, be it in the upgrading of technological means, or the upgrading of the knowledge of human resources.
With the conscience that any effective management would have to be based on profound knowledge of the mechanisms of management, the technologies involved, the configuration of the substructure and the organization of the institution, the learning directives followed in the dissertation had as basis these intentions.
The study carried out culminated with the practical implementation of a system adequate to computing substructure, very rich in technological and system diversity. Some of the presented results of this implementation will reiterate the necessity and advantages of using a management system on the studied substructure.

ÍNDICE

1 Motivação e Enquadramento

1.1 Introdução

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

Quando se levantaram as questões de gestão, na década de 80, elas relacionavam-se essencialmente com as infra-estruturas e equipamentos de comunicação, tendo surgido normas que regulamentavam os mais diversos aspectos desta área. Destas normas fazem parte o *Simple Network Management Protocol* (SNMP), que por ser uma arquitectura aberta e simples de implementar, ainda hoje é utilizado como o principal mecanismo de gestão da quase totalidade dos equipamentos de comunicação e numa quantidade significativa de sistemas de gestão existentes no mercado. Outras tentativas de normalização surgiram entretanto mas tardaram em vigorar e apenas o SNMP vingou, tendo sido alvo de várias actualizações que o tornaram mais robusto e seguro e que o mantiveram actual.

No final da década de 80 o mercado, que era dominado pelos grandes sistemas centrais, assistiu a uma mudança radical de filosofia, com o surgimento dos computadores pessoais cujo abaixamento de preço fez explodir a sua utilização, sendo actualmente o meio computacional dominante no mercado. Esta reviravolta criou a necessidade de uma nova estratégia na abordagem da problemática da gestão, obrigando à construção de mecanismos e normas de gestão mais ricos nas suas funcionalidades e adaptados a este novo cenário. Assim, surgiram várias iniciativas lideradas pelos principais fabricantes de hardware e software, que constituíram fóruns de normalização visando os propósitos descritos.

À gestão de sistemas, num ambiente distribuído, acrescem novos problemas que passam pela actualização do software, pela monitorização e controlo remoto dos sistemas, pela gestão das licenças, pelo 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. Das várias iniciativas nesta área destaca-se o *Web Based Enterprise Management* (WBEM), que pretende constituir uma base de dados única com informação de gestão de toda a infra-estrutura de informática, manipulada através de qualquer dos mecanismos de gestão disponíveis.

Também a gestão de redes foi evoluindo deparando-se com novos desafios, como sejam o controlo de qualidade de serviço, diferenciação de tráfego e o suporte multifacetado de serviços a que as actuais redes de dados têm sido sujeitas.

Tendo em conta que a gestão tem por objectivos tornar eficientes e efectivos os recursos de informática para a Instituição em geral e para os utilizadores em particular, para além de todas as questões técnicas relacionadas com sistema de gestão a implementar existe um outro factor que não pode ser negligenciado na gestão de uma infra-estrutura de

informática, que se prende com a aptidão e disponibilidade dos utilizadores para o uso das novas tecnologias. Este factor é dependente do ambiente de trabalho e da própria orgânica da Instituição, pelo que a sua análise e solução podem assumir níveis de complexidade muito elevados.

Face a todas as questões expostas a gestão de uma infra-estrutura de informática é, com certeza, uma tarefa complexa, estando dependente não só dos meios tecnológicos existentes, mas também e sobretudo, de técnicos especializados e da 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

O presente trabalho pretende estabelecer uma série de requisitos, estudar e identificar as soluções de mercado que melhor lhes respondem, proceder à implementação das soluções encontradas e analisar o resultado e aplicabilidade, da solução encontrada, a um cenário real, no caso, a infra-estrutura de informática da Universidade de Aveiro.

1.3 Estrutura

O presente documento encontra-se estruturado em 4 capítulos, para além deste, organizados do modo que se descreve de seguida.

No capítulo 2 serão abordadas, de uma forma bastante resumida, as principais arquitecturas de gestão de redes e as arquitecturas emergentes de gestão de sistemas que têm pautado a evolução deste mercado.

No capítulo 3 será efectuado um estudo de mercado, onde serão identificadas várias plataformas e aplicações, quer da área da gestão de redes, quer da área da gestão de sistemas, bem como as suas características principais, que serão ponderadas na constituição da plataforma de gestão pretendida.

No capítulo 4 será apresentado o caso de estudo, onde será enquadrada a plataforma de gestão no cenário traçado. Neste capítulo serão abordadas, em detalhe as aplicações que constituirão a plataforma de gestão.

No capítulo 5 serão apresentados os resultados obtidos com a implementação da plataforma, elucidando para as vantagens advindas da utilização de ferramentas de gestão no processo de manutenção de uma infra-estrutura de informática.

No capítulo 6 será feita uma retrospectiva do trabalho realizado, identificando direcções para trabalho futuro com vista a melhorar e complementar as funcionalidades da plataforma de gestão.

1.4 Notação Utilizada

Os termos originais utilizados correntemente, nesta área, pertencem quase sempre à nomenclatura anglo-saxónica, podendo, em alguns casos, a tradução para português ser pouco precisa na significância do termo original. No entanto, ao longo desta dissertação optou-se por efectuar, sempre que possível, a tradução de todos os termos para português, utilizando as traduções já existentes e aproximando, o mais possível, as que ainda não existem, esperando que esta atitude contribua para o enriquecimento do nosso vocabulário técnico. Os termos que forem deixados sem tradução serão colocados em itálico.

Ao longo da dissertação são por vezes utilizados acrónimos, que se encontram devidamente identificados pela utilização de letra maiúscula, com o seu significado descrito na secção de Acrónimos.

No respeitante às referências, elas seguem as directrizes de muitas publicações, sendo constituídas por um conjunto de letras indicativas do autor, seguidas do ano de publicação e podem ser encontradas no texto dentro de parêntesis rectos [...]. Uma lista completa e pormenorizada destas referências pode ser encontrada no final da dissertação.

2 Arquitecturas de Gestão

2.1 Introdução

A análise e resolução dos problemas de gestão podem ter várias aproximações que vão desde o tratamento dos problemas isoladamente até uma visão integrada da infra-estrutura, actuando sobre ela como um todo. Nesta última aproximação, as arquitecturas de gestão têm um papel fundamental, constituindo a base para o desenvolvimento de sistemas de gestão abertos, aplicáveis nos ambientes heterogéneos existentes nas actuais infra-estruturas de informática.

A evolução das arquitecturas de gestão tem acompanhado o crescimento, quer em número, quer em complexidade, dos sistemas e das infra-estruturas no seu todo, tendendo cada vez mais para a existência de arquitecturas integradoras das operações de gestão.

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

2.2 Recursos a Gerir e a Aplicação das Arquitecturas de Gestão

As infra-estruturas de informática actuais são constituídas pelo conjunto de todos os equipamentos, meios de transmissão, aplicações e serviços, que interagem entre si cooperativamente. Estas infra-estruturas são designadas vulgarmente por infra-estruturas de Tecnologia de Informação (TI) e constituem actualmente o suporte e um factor competitivo em todas as actividades do quotidiano em que vivemos. A gestão das infra-estruturas TI apresenta-se, assim, como um factor de importância fundamental em qualquer organização.

Para o presente trabalho importa considerar estas infra-estruturas divididas em dois grandes grupos: as infra-estruturas de comunicações e os sistemas.

As infra-estruturas de comunicações são constituídas pelos equipamentos e pelos meios de transmissão que implementam os níveis 1, 2 e 3 do modelo OSI (Figura 2.1), cujos sistemas de gestão são vulgarmente designados por sistemas de gestão de redes. A variedade dos recursos e tecnologias adjacentes apresentam-se como um desafio ao objectivo de gerir uma infra-estrutura e é notória em todas as áreas: meios de transmissão, equipamentos de comutação e encaminhamento, etc. (Figura 2.1, Figura 2.2).

Na história da Internet podem observar-se dois tipos de redes diferentes, as redes de área local (LANs ou Intranets) e as redes de área alargada WANs. Nestes dois tipos de redes, existem diferenças, quer ao nível dos equipamentos quer ao nível das normas adoptadas. Em relação às LANs e à Internet, as normas que foram adoptadas na sua regulamentação foram as definidas pelo IEEE (série 802.X) e as definidas em RFCs pelo IETF. Relativamente às WANs foram utilizadas, essencialmente, as recomendações da ITU e da

ISO [HST99]. Convém, no entanto, referir que não existem dois mundos estanques mas que, cada vez mais, eles se confundem numa panóplia de tecnologias diversas.

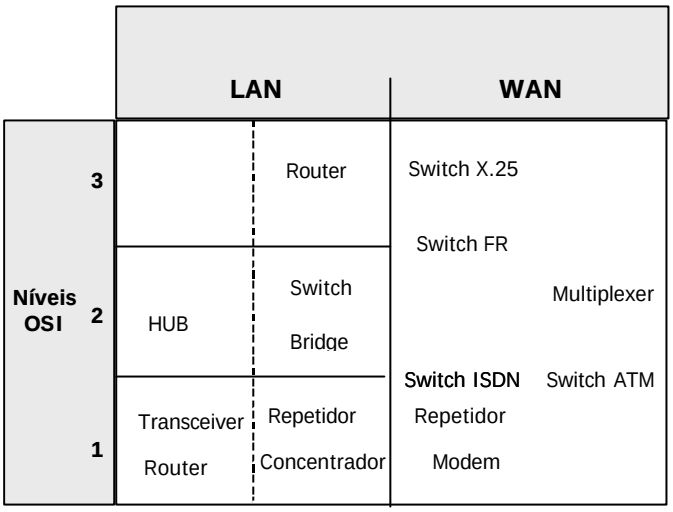


Figura 2.1 – Componentes de uma infra-estrutura de comunicações (baseado em [HSB99]).

As redes de comunicações destinam-se a permitir o estabelecimento de uma comunicação entre duas ou mais partes (sistemas), ou seja, a possibilitar a troca de informação, assumindo um papel fundamental na sociedade actual. A diversidade de tipos de informação (dados, voz, vídeo e, actualmente muito em voga, multimédia) levou a que houvesse uma distinção, até há pouco tempo clara, entre redes de dados e redes e telecomunicações, às quais era associado, respectivamente, o transporte de dados e o transporte de informação de voz e vídeo. Esta fronteira está a desvanecer-se, cada vez mais, sendo exemplos disso a voz sobre IP, que possibilita constituir uma rede de voz sobre uma rede de dados, ou as aplicações multimédia que fazem uso das tecnologias de transferência de dados para trocar informação quer de dados, quer de voz e vídeo. A somar a estes factores, as recentes evoluções no domínio dos sistemas distribuídos têm feito das redes de dados o fundamento para o sucesso de qualquer sector do mercado, apresentando, por outro lado, novos desafios à implementação dos modelos de gestão.

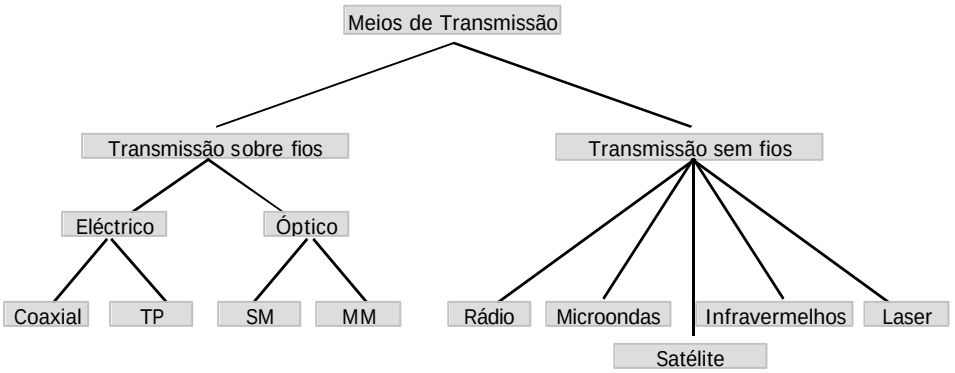


Figura 2.2 – Meios de transmissão mais comuns (baseado em [HSB99]).

Esta diversidade, ilustrada na Figura 2.3, vem reforçar ainda mais a importância de criar, e essencialmente adoptar, normas que permitam constituir sistemas de gestão integrados.

Sendo a arquitectura TCP/IP a mais utilizada o seu modelo de gestão é também o mais popular. Comparativamente ao modelo OSI, os conceitos são significativamente mais simples, pelo que permitem a sua implementação em equipamento com menores capacidades computacionais e com custos associados mais baixos. A adopção generalizada deste modelo pelos vários fabricantes proporcionou a criação de plataformas de gestão compatíveis com os múltiplos equipamentos dos fabricantes.

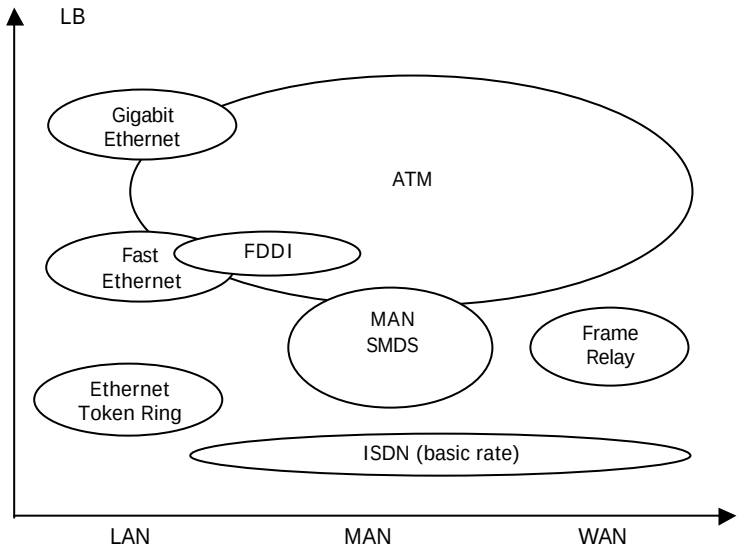


Figura 2.3 – Tecnologias de redes de comunicações (baseado em [HSB99]).

As arquitecturas das redes de dados, que têm normalmente associado um modelo de gestão, são caracterizadas por um conjunto de protocolos que definem o seu funcionamento e constituem a base para o estabelecimento de interfaces de cooperação entre as várias tecnologias existentes, sendo a arquitectura OSI um modelo de referência e a arquitectura TCP/IP a mais utilizada nas redes de dados.

Estes sistemas, que durante cerca de uma década foram os únicos existentes no mercado, são agora complementados por arquitecturas semanticamente mais ricas e elaboradas que são a base da gestão de sistemas.

No que respeita aos sistemas, até há pouco tempo a sua filosofia não suscitava necessidades de gestão integrada, mas o aparecimento dos PCs e a deslocação do processamento e das aplicações para os computadores pessoais, levantaram essa necessidade, para a qual os fabricantes têm tentado dar uma resposta coerente e uniforme.

Nos últimos anos tem-se assistido ao crescimento das infra-estruturas de informática com um protagonismo dos sistemas distribuídos, para as quais os modelos de gestão tradicionais apresentam algumas limitações. As limitações dos modelos de gestão de redes, encontram-se ao nível da simplicidade e semântica pouco rica que não permitem modelar

adequadamente as variáveis associadas à gestão de sistemas, criando a necessidade de concepção de novos modelos, dos quais são exemplos o DMI e o WBEM.

As novas tecnologias para gestão de sistemas têm proporcionado mecanismos de extrema importância, nas actuais infra-estruturas, que passam pela distribuição de software, controlo remoto, inventariação de hardware e software, em suma mecanismos que suavizam as tarefas de manutenção de uma infra-estrutura [DDR00].

Também nestes sistemas, a pluralidade de recursos é igualmente grande, apesar de algum domínio dos sistemas Microsoft e das plataformas Intel, sendo os mecanismos de gestão constituídos em redor destas tecnologias. A discussão que se centrava sobre as tecnologias de gestão de redes e sistemas começa agora a deslocar-se para a área do negócio, sendo cada vez mais estratégica a discussão destas questões do ponto de vista da área de negócio da instituição [JHE99]. A gestão das infra-estruturas TI apresenta-se assim, como um factor de importância fundamental em qualquer organização, subdividida em vários níveis complementares e que podem ser endereçados individualmente, entre os quais se encontra a rede e os sistemas (Figura 2.4).

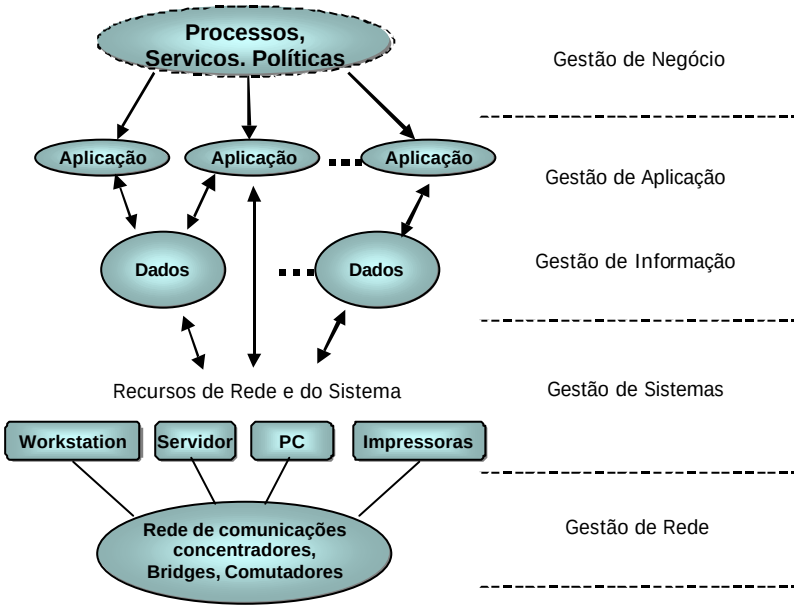


Figura 2.4 – Os níveis da gestão integrada (baseado em [HSB99]).

É de referir também o papel, cada vez mais importante, atribuído aos processos e mecanismos de gestão baseados numa estrutura de directórios, como o DEN, que apresentam inúmeras vantagens na gestão centralizada e organizada de uma instituição [ARA00a].

Por último, e para além de não ser objecto de estudo neste trabalho, que se irá restringir à gestão da infra-estrutura de comunicações e à manutenção de sistemas, a gestão da informação no que respeita à segurança e ao armazenamento é um assunto que assumiu

uma importância tal que não pode ser deixado de parte no projecto de uma infra-estrutura de informática.

2.3 Modelos de Gestão de Rede

A gestão encontra-se, conceptualmente, divida em áreas funcionais, que podem ou não estar todas incluídas num mesmo sistema de gestão. As áreas funcionais, propostas pela ISO, são 5: gestão de falhas, gestão de configuração, gestão de contabilidade de utilização, gestão de desempenho e gestão de segurança [ISO/IEC 10164] [ITU-T X.700]. Estas áreas funcionais são normalmente designadas por FCAPS, as inicias dos correspondentes termos em inglês [HSB99], em português: gestão de falhas *(Fault)*, gestão de configuração *(Configuration)*, gestão de contabilização *(Accounting)*, gestão de desempenho *(Performance)* e gestão de segurança *(Security)* [DTP99].

As áreas funcionais são endereçadas pelos dois modelos de gestão, o modelo OSI e o modelo TCP/IP, que protagonizam a referência na actual gestão das infra-estruturas de comunicações.

2.3.1 Modelo OSI

O modelo de referência *Open Systems Interconnection* (OSI), definido pela *International Organization for Standardization* (ISO), deve a sua importância ao facto de ter sido desenvolvido por um organismo internacional de normalização, constituindo assim, uma referência na adopção de normas relativas a redes de comunicações. A mais valia obtida com a possibilidade de constituir sistemas globalmente normalizados esbarra com a complexidade de implementação de sistemas baseados num modelo complexo como o OSI e com a globalização de um outro modelo concorrente, o modelo TCP/IP. A utilização do modelo OSI assume maior importância nas redes de telecomunicações. Nas redes de dados, a referência a este modelo dificilmente é encontrada. No entanto, tem constituído uma boa base de trabalho para as tecnologias emergentes.

O modelo de referência OSI encontra-se subdividido em 7 camadas distintas, das quais algumas se aplicam, com maior ou menor extensão a toda a Internet. Estas camadas isolam, para as camadas superiores, os pormenores de implementação das camadas inferiores, o que facilita o desenvolvimento aplicacional a vários níveis. As funções principais das várias camadas são representadas na Figura 2.5 e descritas de seguida:

- **Camada física:** Esta camada é responsável pelo funcionamento transparente do transporte dos bits através dos vários meios físicos (cobre, fibra óptica, rádio, etc), sendo ainda responsável pelos processos de codificação e modulação.
- **Camada lógica:** Pode ser dividida em duas sub-camadas, a camada de acesso ao meio de transmissão, responsável pelo acesso dos vários participantes na comunicação, ao mesmo meio físico partilhado. No caso das LANs, esta sub-camada implementa os procedimentos de alocação e reserva de recursos, fazendo

parte dele a Ethernet – IEEE 802.3, a Token Ring – IEEE 802.5 e o FDDI – ANSI X.3T9.5 e ISO 9314. A segunda sub-camada, a *Logical Link Layer* (LLC), assume, quando existe, as funções de controlo de erros e agrupamento de bits em mensagens.

- **Camada de rede:** Esta camada é responsável pelo encaminhamento das ligações lógicas, fazendo parte dela os mecanismos de comutação e encaminhamento da informação.
- **Camada de transporte:** providencia, a dois sistemas terminais, uma interface independente da camada de rede, permitindo-lhes requisitar determinados parâmetros da rede, tais como: taxa de transmissão, taxa de erros, atraso,... O estabelecimento de ligações orientadas ao pacote e à conexão também é efectuado neste nível.
- **Camada de sessão:** estabelece, estrutura e controla as sessões, providenciando para os níveis superiores mecanismos de controlo e configuração dessas sessões, que têm carácter temporário.
- **Camada de apresentação:** garante, para as aplicações, uma linguagem de diálogo única e normalizada. Isto significa que as partes envolvidas dialogam num determinado contexto e representam os dados segundo um mesmo formato. No sentido lato, este nível é responsável por garantir a mesma interpretação da informação.
- **A camada de aplicação**: sendo responsável pela interface com o utilizador, contém as aplicações propriamente ditas e deve ser totalmente independente das camadas inferiores.

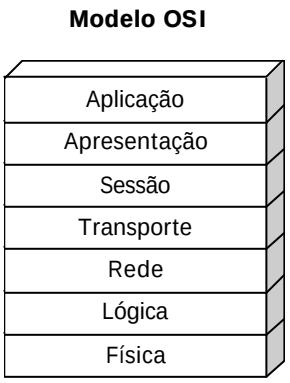


Figura 2.5 – Níveis do modelo OSI.

O modelo OSI tem associado um modelo de gestão, baseado no *Common Management Information Protocol* (CMIP). Este modelo é, no entanto, bastante mais complexo que o modelo TCP/IP (ou SNMP) e não teve um impacto muito grande junto dos fabricantes e empresas.

2.3.2 Modelo TCP/IP

As origens do TCP/IP remontam ao final 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 dos documentos, *Request for Comments* (RFCs), que passaram a definir a pilha protocolar TCP/IP. Até meados de 1980 a utilização do TCP/IP e da Internet, era quase limitada aos organismos militares e de educação. A partir dos anos 90, em que começaram os esforços por desenvolver normas internacionais com o modelo OSI, deu-se também o crescimento desenfreado da Internet em ambiente comerciais, o que aumentou significativamente a importância das soluções de gestão para a própria rede.

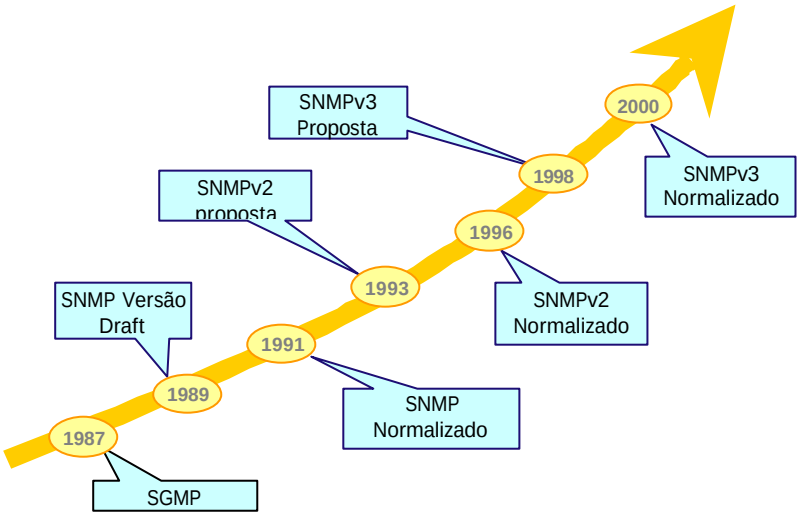


Figura 2.6 – Evolução do SNMP.

A arquitectura protocolar TCP/IP possui, neste momento, uma posição dominante no mercado das redes de comunicações de dados, sendo o modelo utilizado na Internet.

Por detrás desta conjuntura esteve um organismo de normalização aberto, o *Internet Engineering Task Force* (IETF), constituído por representantes de várias entidades e empresas do sector, que fomentaram e fomentam o debate público, através de *Request for Comments* (RFC) e aprovaram as normas aplicáveis nas redes IP. As normas daqui resultantes são sempre soluções consensuais e muitas vezes com provas dadas no mercado, o que facilita a sua implementação generalizada.

A descrição do modelo Internet pode ser feita, por comparação com o modelo OSI, facilitando e simplificando a sua análise (Figura 2.7).

As funções básicas desempenhadas por cada modelo são idênticas. No entanto, o modelo Internet encontra-se subdividido de um modo ligeiramente diferente, dispondo-se apenas em 4 camadas distintas.

- **Camada de acesso ao meio:** tem correspondência com as camadas 1 e 2 do modelo OSI e é responsável pela interface com os meios físicos de transmissão.
- **Camada de rede (internet):** esta camada é a responsável pelas funções básicas de comunicação, nomeadamente endereçamento, encaminhamento e comutação. A importância desta camada é vital, ela pode mesmo ser vista como o coração da Internet, já que é a responsável por todo o encaminhamento.
- **Camada de transporte:** é responsável por manter e controlar as sessões, detectar erros e efectuar retransmissões caso seja necessário.
- **Camada de aplicação:** No modelo Internet, e por comparação com o modelo OSI, não existe uma distinção clara entre os níveis 5, 6 e 7, sendo as funções correspondentes asseguradas nesta camada.

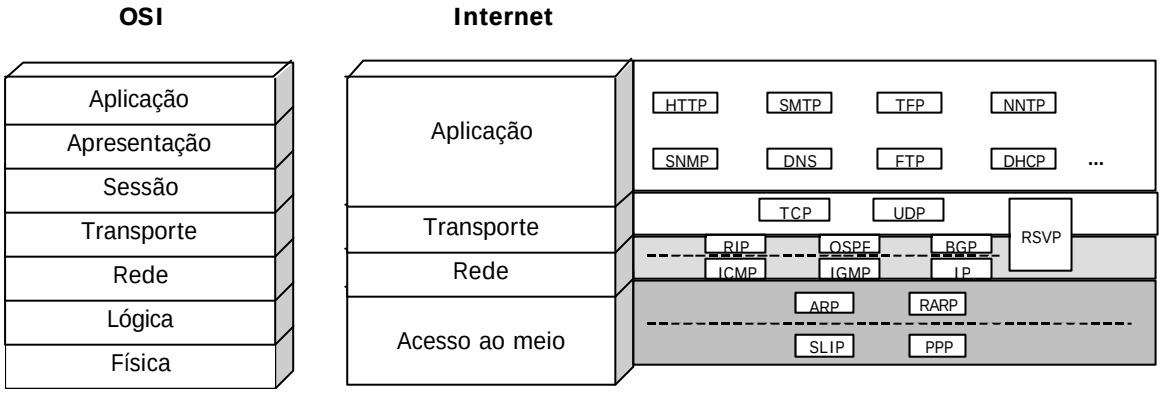


Figura 2.7 – Modelo OSI vs Internet.

A Figura 2.7 representa alguns dos protocolos utilizados em cada camada do modelo, apresentando diferentes facilidades e mecanismos que respondem às diferentes solicitações de serviço efectuadas pelas camadas superiores.

2.3.2.1 Simple Network Management Protocol (SNMP)

A necessidade de mecanismos de gestão levou à criação de várias propostas para normas de gestão entre elas o *Host Monitoring Protocol* (HMP), o *Simple Gateway Monitoring Protocol* (SGMP) e o CMOT (CMIP sobre TCP/IP) que, posteriormente, iriam evoluir para o SNMP [RFC1157]. Em 1988, o IAB, adoptou o SNMP como mecanismo de gestão a curto prazo, que seria substituído pelo CMOT cuja abrangência de funções era muito superior, mas dada a sua complexidade teria uma fase de implantação mais lenta. A relutância na implementação do SNMP era grande, porque a entrada no mercado do CMOT iria pôr em causa todo o trabalho realizado tendo por base o SNMP. Na tentativa de colmatar este problema, e uma vez que o CMOT teimava em demorar, optou-se pela

criação de uma estrutura de informação idêntica para os dois modelos, variando apenas as aplicações e os protocolos utilizados. No entanto, rapidamente se concluiu que esta estratégia era impraticável, já que os objectos do modelo OSI eram muito complexos com atributos, variáveis e outros parâmetros, ao passo que na simplicidade do SNMP, os objectos não passam de meras variáveis com algumas características.

Depois da separação dos dois grupos de trabalho, o desenvolvimento do SNMP teve um desenrolar semelhante ao do TCP/IP, enquanto o esforço de desenvolvimento do CMOT continuava a ser limitado. Rapidamente o SNMP se tornou no protocolo de gestão de excelência da Internet, sendo adoptado pela maioria dos fabricantes de equipamento de rede. A Figura 2.6 pretende mostrar a sua evolução até aos dias de hoje.

Existe um conjunto de normas relacionadas com o SNMP e as suas evoluções que definem totalmente o seu funcionamento (Tabela 2.1). Alguns destes documentos sofreram já várias revisões tendo sido substituídos por outros, no seguimento de uma política de acompanhamento das necessidades e evolução tecnológica.

Tabela 2.1 – RFCs em uso na arquitectura SNMP [IETF].

RFC	Data	Estado	Titulo
1155	Maio, 1990	full	Structure and Identification of Management Information for TCP/IP-based Internets
1157	Maio, 1990	full	A Simple Network Management Protocol (SNMP)
1212	Março, 1991	full	Concise MIB Definitions
1215	Março, 1991	full	A Convention for Defining Traps for use with the SNMP
1901	Janeiro, 1996	experimental	Introduction to Community-based SNMPv2
1902	Janeiro, 1996	draft	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
1903	Janeiro, 1996	draft	Textual Conventions for Version 2 of Simple Network Management Protocol (SNMPv2)
1904	Janeiro, 1996	draft	Conformance Statements for Version 2 of Simple Network Management Protocol (SNMPv2)
1905	Janeiro, 1996	experimental	Protocol for Version 2 of Simple Network Management Protocol (SNMPv2)
1906	Janeiro, 1996	experimental	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
1909	Fevereiro, 1996	experimental	An Administrative Infrastructure for SNMPv2
1910	Fevereiro, 1996	experimental	User-based Security Model for SNMPv2
2261	Janeiro, 1998	proposed	An Architecture for Describing SNMP Management Frameworks
2262	Janeiro, 1998	proposed	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
2263	Janeiro, 1998	proposed	SNMPv3 Applications
2264	Janeiro, 1998	proposed	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
2265	Janeiro, 1998	proposed	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

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 2.8): Estação de Gestão (1), Agente (2), Protocolo de Gestão (3) e Base de Informação de Gestão (MIB) (4).

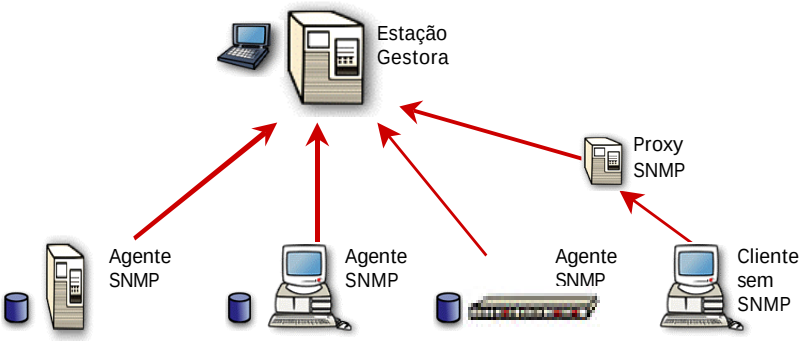


Figura 2.8 – Funcionamento do SNMP.

A MIB é disponibilizada pelo agente à estação de gestão, sendo a comunicação estabelecida através de um protocolo (SNMP), que suporta primitivas básicas para a troca de informação entre as duas entidades (Figura 2.9). Esta informação, acedida através do SNMP, é a base de funcionamento da maioria das aplicações de gestão de redes.

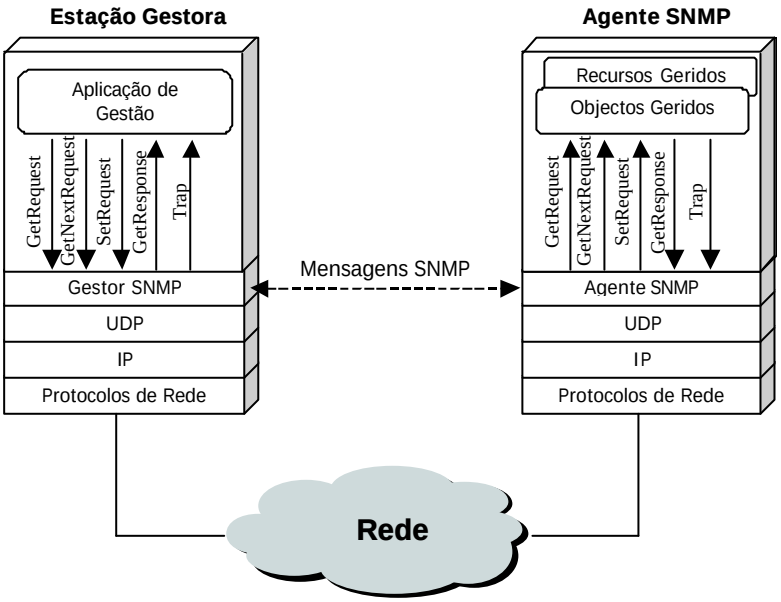


Figura 2.9 – Arquitectura do SNMP.

Com a publicação da versão 3, o SNMP é finalmente contemplado com mecanismos de segurança, cuja ausência, apesar da larga implementação desta arquitectura no mercado, sempre foi um factor em seu desfavor. 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 [RFC1905,06,09,10]. A implementação dos mecanismos de segurança aproveita os formatos de mensagem das anteriores versões (Figura 2.10).

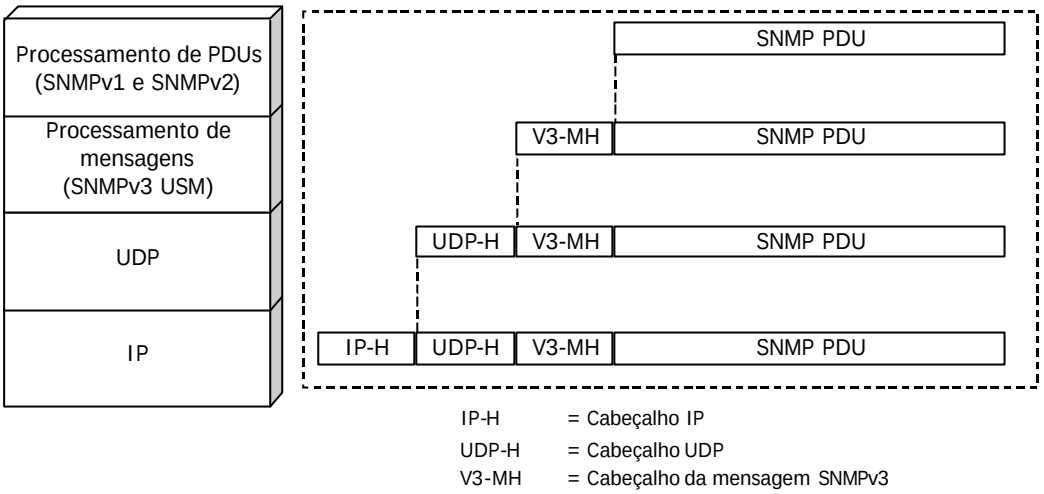


Figura 2.10 – Arquitectura protocolar do SNMPv3.

A arquitectura do SNMPv3 [RFC2271] foi desenvolvida segundo módulos, tendo em vista o posterior aperfeiçoamento de cada módulo de forma independente (Figura 2.11). Relativamente à segurança são contemplados dois modelos: o *User Security Model* (USM) [RFC2274] e o *View-based Access Control Model* (VCAM) [RFC2275].

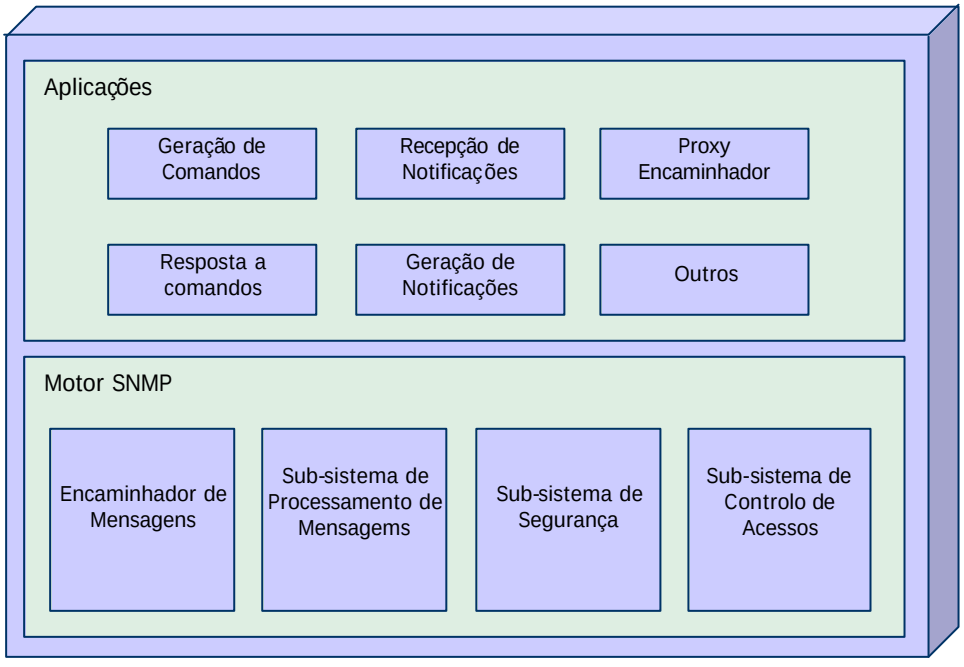


Figura 2.11 – Entidade SNMP.

Uma entidade SNMP é constituída por um motor SNMP, que é único nessa entidade, e uma série de funções responsáveis pelos serviços de tratamento de mensagens, controlo de acesso, autenticação e criptografia das mensagens [JJA98]. O papel desempenhado por

uma entidade SNMP é definido pelos módulos que 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 revisão de toda a norma.

O SNMP funciona numa filosofia cliente-servidor onde a estação gestora recolhe a informação proveniente dos vários agentes, os quais podem ser implementados nos mais diversos equipamentos fornecendo informação genérica e normalizada utilizada pelas plataformas de gestão base, ou então proprietária do fabricante e utilizada pelas suas próprias aplicações. Numa rede não é necessário que todos os equipamentos implementem um agente SNMP, desde que haja alguns deles com as funções de proxy e que forneçam informação sobre os primeiros.

2.3.2.2 Management Information Base (MIB)

O modelo de gestão define a sua própria estrutura da informação, a qual designa por *Structure of Management Information* (SMI) [RFC1155], sendo a base para a especificação da Informação de Gestão (MIB). A semântica definida pela SMI apresenta a informação segundo uma estrutura em árvore, como representado na Figura 2.12.

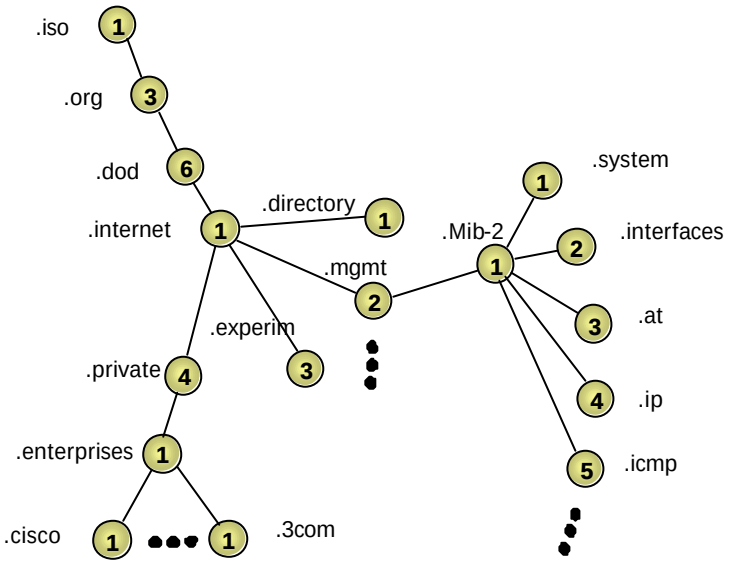


Figura 2.12 – Estrutura da organização da informação.

Os objectos, ou variáveis, das MIBs são definidos formalmente na notação ASN.1 [ISO8824] e são identificados univocamente através de uma sequência de inteiros, apresentando por exemplo o formato .1.3.6.1.2.1.1 para identificar o objecto *system* da MIB-2. A linguagem ASN.1 é utilizada também para definir os *Protocol Data Unit* (PDUs), utilizados pelo SNMP na comunicação entre a estação gestora e o agente SNMP.

Quando surgiu, a MIB-I, uma base genérica para qualquer agente, apresentava um limite predeterminado de 100 objectos, com o objectivo de permitir a todos os fabricantes a

instrumentação dos seus equipamentos com base nesses objectos. A MIB-II que lhe sucedeu, tendo em conta o crescimento tecnológico existente nos equipamentos de rede, passou a conter um conjunto bastante mais amplo de variáveis, agrupadas pelas suas características, nos grupos: *system, interfaces, at, ip, icmp, tcp, udp, egp, transmission, snmp* [MIB-II]. Estas variáveis fornecem um vasto conjunto de informação, essencialmente, sobre as interfaces dos equipamentos e constituem a base de informação das aplicações de gestão generalistas.

Após a MIB-I e MIB-II muitas outras especificações foram propostas visando reflectir melhor as características particulares de cada equipamento de rede ou de cada tecnologia. De entre estas destacam-se a *Remote Monitoring MIB* (RMON) pela sua importância na monitorização de rede, isto é, por ser uma MIB que recolhe informação de rede e não informação do sistema.

2.3.2.3 Remote Monitoring (RMON) MIB

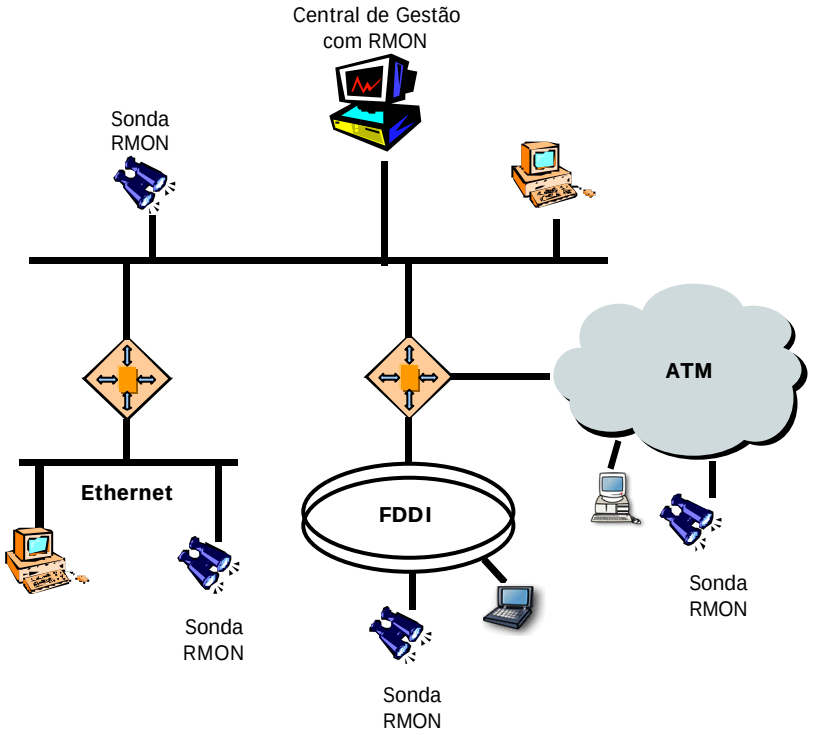


Figura 2.13 – Configuração da monitorização RMON.

A RMON MIB surgiu como uma solução que permite, ao agente, recolher informação respeitante ao troço de rede onde está inserido e aos nós que lhe são adjacentes (Figura 2.13). A implementação RMON propunha-se alcançar alguns objectivos, que proporcionariam uma gestão mais flexível, entre eles: a recolha de informação sem estar ligado à estação gestora, monitorização constante de variáveis e ocorrências predeterminadas, gestão activa através de notificações geradas pela ocorrência de

determinados eventos, determinação das variáveis a analisar na recolha de informação do troço de rede e a disponibilidade da informação para várias estações de gestão [DTP99].

A primeira especificação de agentes RMON foi efectuada em 1991 com o RFC 1271, seguidamente foi elaborado o RFC1523 que define as extensões para monitorização remota de *Token Ring* e o RFC1757 que tornou obsoleto o RFC1271 e é actualmente utilizado como referência.

O RMON herdou a simplicidade e os mecanismos utilizados pelo SNMP, na medida em que se trata apenas da definição de mais uma MIB, acrescentando um conjunto de funcionalidades que potenciam uma monitorização efectiva dos troços onde as sondas se encontram inseridas. A MIB RMON está dividida em 10 grupos: *statistics, history, alarm, host, hostTopN, matrix, filter, capture, event, tokenRing* [RFC1757].

No mercado actual, as funcionalidades RMON podem ser encontradas embebidas nos equipamentos de interligação (encaminhadores, comutadores, repetidores), em hardware dedicado (sondas) ou em sondas implementadas em software que são executadas num computador, variando no número de grupos implementados.

2.3.2.4 Remote Monitoring MIB versão 2 (RMON2)

A monitorização de informação relativa às camadas 3 a 7 do modelo OSI, só passa a ser possível com a implementação do RMON2 [RFC2021], iniciada em 1994. Esta nova abordagem permite a identificação, não só das máquinas que originam o tráfego, mas também quais as aplicações responsáveis por esse tráfego e a largura de banda ocupada por cada aplicação, perspectivando possíveis arranjos na organização dos servidores e dos clientes ou mesmo na própria infra-estrutura [RMON2].

O RMON2 define mais 9 grupos: *protocolDir, protocolDist, addressMap, nlHost, nlMatrix, alHost, alMatrix, usrHistory, probeConfig*. Com estes grupos passa a ser possível monitorizar os serviços e a largura de banda que eles ocupam, o tipo de tráfego provocado por cada um, etc. No entanto, estas facilidades acrescidas requerem mais memória e um maior poder computacional das sondas, fazendo subir o seu preço.

Na Figura 2.14 é possível observar e comparar as estruturas das MIBs RMON e RMON2 segundo a organização SMI.

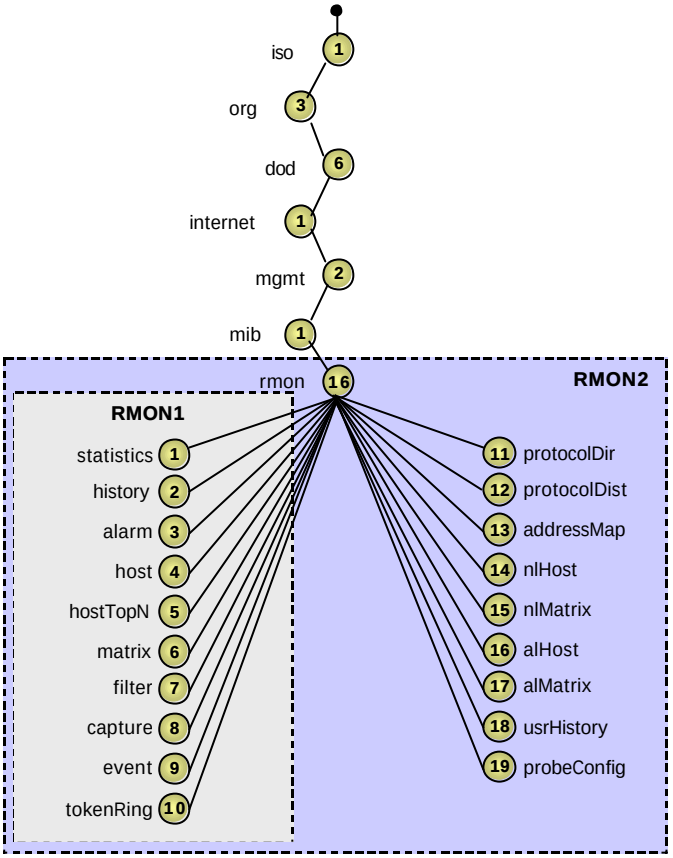


Figura 2.14 – Estrutura da MIB RMON2.

2.4 Modelos de Gestão de Sistemas

A gestão de sistemas, pelas suas particularidades e exigências, levou à criação de modelos próprios. Nesta secção serão descritos alguns destes modelos, ou antes, iniciativas que continuam em desenvolvimento mas que já são largamente adoptadas pelos fabricantes de hardware e software.

2.4.1 Desktop Management Interface (DMI)

Enquanto o SNMP era utilizado para a gestão da infra-estrutura de rede e de equipamentos centrais, aplicações proprietárias eram desenvolvidas para proceder à gestão de servidores e sistemas terminais (PCs). Para colmatar este problema o *Desktop Management Task Force* (DMTF) criou em 1994 a especificação do DMI 1.0 que pretendia tornar os servidores, os portáteis e os desktops geríveis independentemente do hardware e do sistema operativo neles instalado.

O DMI foi especificado de modo a que todos os componentes dos sistemas, hardware (board, discos, fontes de alimentação, placas de rede,...) e software (drivers, aplicações,...), implementassem esta norma, possibilitando o diagnóstico e configuração remota de todos os componentes instrumentados, sendo estes mecanismos disponibilizados pelo provedor de serviços (*Service Provider* – SP). Na prática o funcionamento do DMI é muito

semelhante ao do SNMP, sendo implementadas pelos provedores de serviços bases de informação que são disponibilizadas à estação gestora (Figura 2.15, Figura 2.16).

Figura 2.15 – Funcionamento do DMI.

O *Desktop Management Task Force* (DMTF) publicou várias versões do DMI, a versão 1.0 abordava o problema da implementação local da norma ao nível dos equipamentos a gerir (PCs, Impressoras, equipamentos de rede,...) e a compatibilidade com tecnologias existentes, nomeadamente o SNMP. O DMI 2.0 [DMTF98] vem endereçar a gestão remota de sistemas com suporte DMI através de mecanismos de *Remote Procedure Call* (RPC) [ONG706].

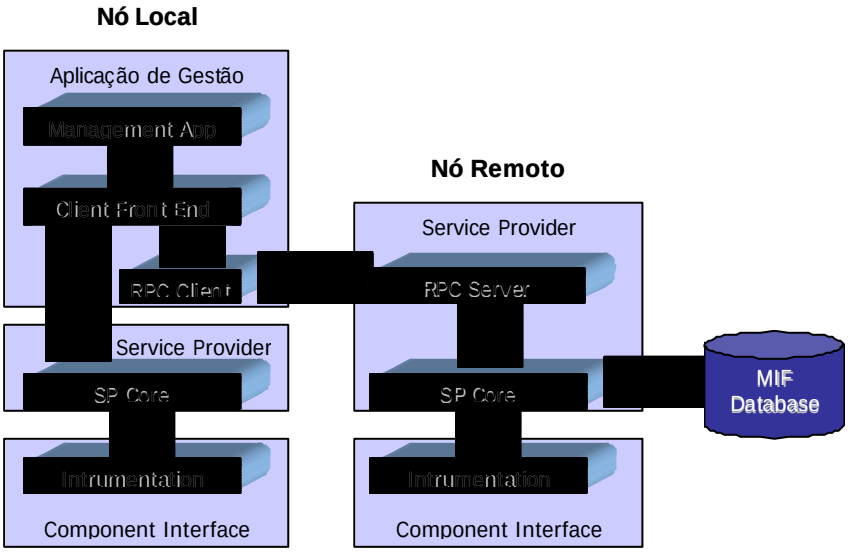


Figura 2.16 – Comunicação DMI.

O DMI define uma camada, *Service Provider* (SP), que medeia a troca de informação entre a aplicação de gestão *Management Interface* (MI) e o elemento gerido *Component Interface* (CI).

O provedor de serviços utiliza uma base de dados, a *Management Information Format* (MIF) para armazenar os dados relativos a cada componente instrumentado (Figura 2.17).

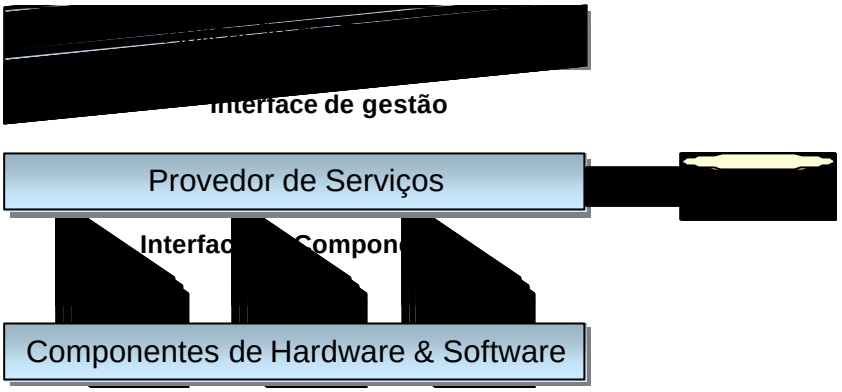


Figura 2.17 – Modelo Funcional do DMI.

Cada componente possui uma MIF que descreve os vários atributos organizados em grupos. Quando um componente é instalado num sistema a sua MIF é adicionada à MIF do sistema, e ao contrário do que acontece no SNMP não é necessário que estação gestora carregue também a MIF para poder fazer a navegação da MIF e efectuar tarefas de gestão.

O funcionamento do DMI é muito semelhante ao do SNMP no que diz respeito à estrutura da informação e às entidades envolvidas, tendo sido especificados mapeamentos entre as duas tecnologias visando a manipulação dos dados por uma única aplicação. Estes mapeamentos podem ser implementados por agentes no cliente ou na estação gestora, convertendo a informação DMI em SNMP ou vice-versa.

2.4.2 Java Management Extensions (JMX)

A iniciativa JMX, promovida pela SUN, surgiu com o nome de *Java Management API* (JMAPI) em 1996, tendo evoluído em 1999 para o JMX, no seguimento das especificações do JMAPI 2.0. O JMX define uma infra-estrutura onde podem ser adicionados, on-line, componentes auto-descritivos, que possibilitam uma modelação dinâmica do sistema de gestão. A arquitectura do JMX[SUN99a] encontra-se dividida em três níveis distintos: instrumentação, agente e gestor (Figura 2.18)

O nível de instrumentação providencia os mecanismos de gestão para qualquer objecto, podendo ser implementado nativamente em Java ou implementado um adaptador. O nível agente é composto por um conjunto de *Management Beans* (MBeans) que representam os objectos geridos, podendo ser registados no servidor MBean que através de interfaces baseadas em Java, desencadeia todas as operações de gestão sobre os objectos.

Os adaptadores de protocolos possibilitam que as operações de gestão sejam efectuadas através de outro protocolo como o SNMP ou HTTP. Finalmente o nível gestor providencia um conjunto de componentes que permitem operar com os agentes, podendo utilizar qualquer protocolo suportado. Uma das preocupações do JMX é a integração com os modelos existentes, pelo que existe um conjunto de APIs, que permitem integrar o JMX com SNMP, CIM/WBEM, TMN, CORBA e LDAP [SUN00a].

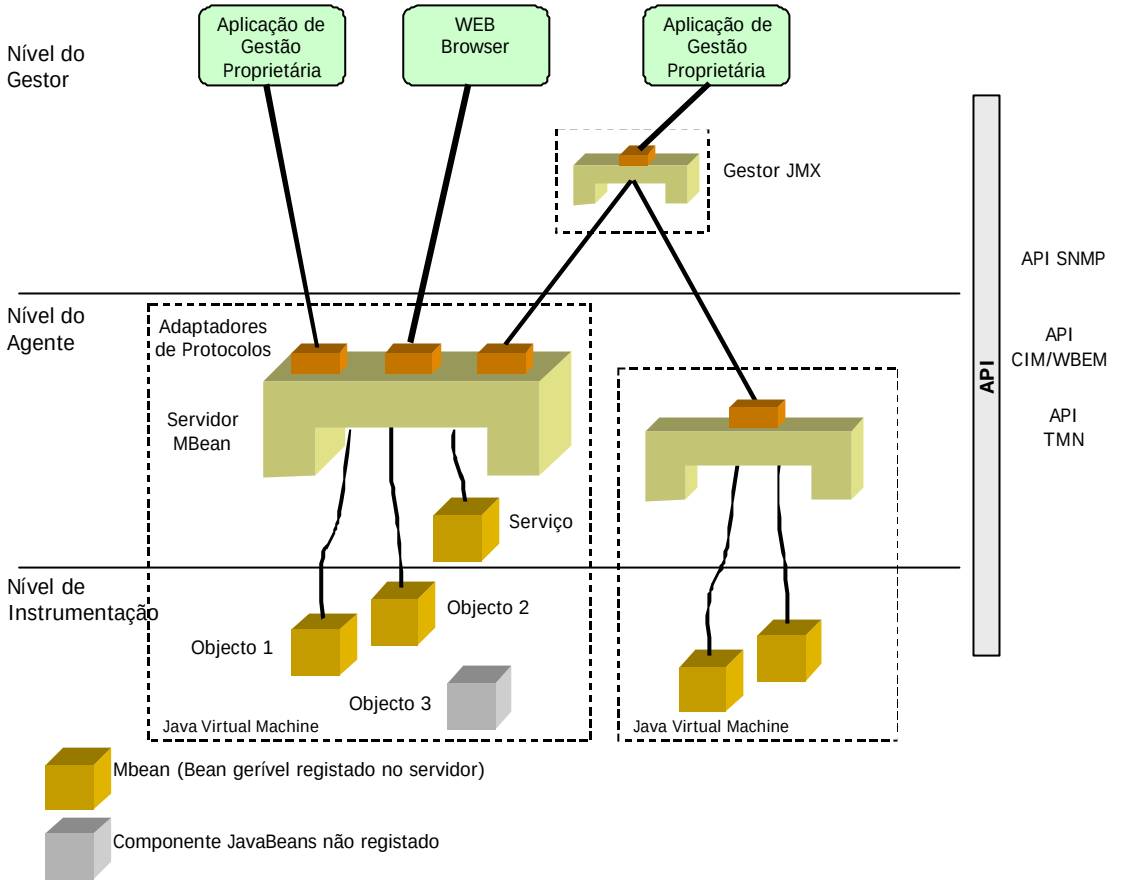


Figura 2.18 – Arquitectura do JMX (baseado em [SUN00a]).

Esta iniciativa é encabeçada pela SUN, no seguimento da popularidade da linguagem JAVA e não tem por enquanto qualquer suporte nos organismos de normalização.

2.4.3 Web Based Enterprise Management (WBEM)

O WBEM surge mais ou menos na mesma altura que o JMAPI e propõe-se aproveitar a vulgarização de tecnologias Internet para a criação de mecanismos de gestão, acessíveis em qualquer momento, a partir de qualquer local, de preferência com uma interface de configuração e gestão única, o que facilita a tarefa de aprendizagem da manutenção. A evolução das tecnologias Web vem marcar um rumo no desenvolvimento desta ideia, que passa pela utilização de um browser Web para proceder à gestão de todos os sistemas (Figura 2.19).

Combinando as tecnologias de gestão já existentes com novas funcionalidades introduzidas, o WBEM faz uma renovada abordagem da gestão, passando de uma aproximação de duas camadas para uma aproximação de três camadas (Figura 2.22) onde a nova camada faz a adaptação das várias tecnologias para uma interface comum.

Figura 2.19 – Gestão baseada na Web.

A iniciativa WBEM teve origem em meados de 1996 (Figura 2.20) e foi liderada pela Intel, Microsoft, CISCO e Compaq. Esta iniciativa começou por ser uma base de trabalho para sistemas de gestão baseados em tecnologia orientada a objectos, mas tem agora como grande objectivos, proceder à integração de normas como o SNMP, DMI e o CMIP, unificando o acesso à informação de modo a utilizar um único interface para efectuar a gestão [JTU00]. Actualmente, esta interface é sem dúvida o browser WEB, sendo inclusivamente já disponibilizada em muitos equipamentos de comunicações e sistemas terminais.

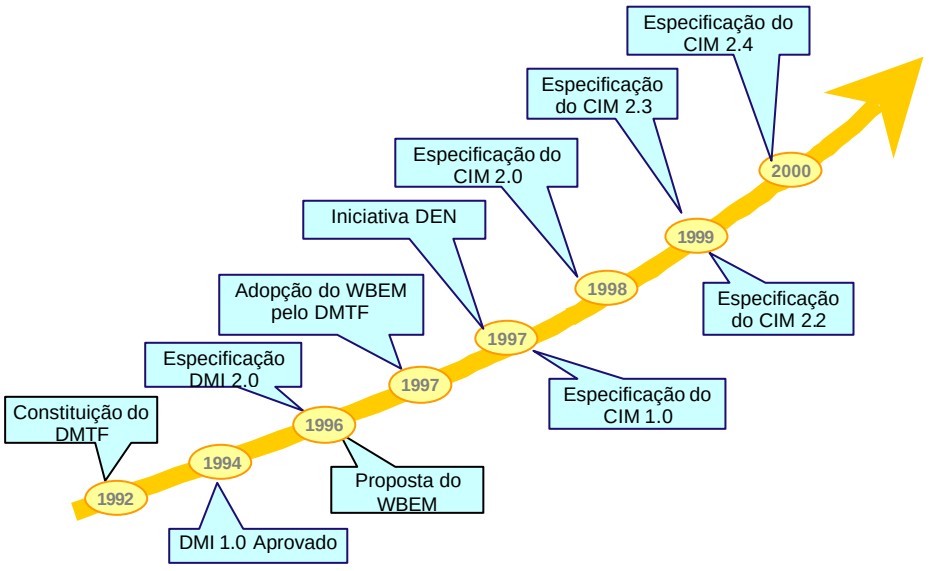


Figura 2.20 – Evolução das tecnologias de gestão de sistemas.

O modelo de informação é o *Common Information Model* (CIM), definindo uma estrutura que permite a partilha de dados entre aplicações, por exemplo usando o *extensible markup language* (XML) que facilita o acesso através de HTTP, integrando informação de gestão

SNMP, DMI e CMIP, com um esquema expansível e adaptável ao ambiente de rede da organização (Figura 2.21).

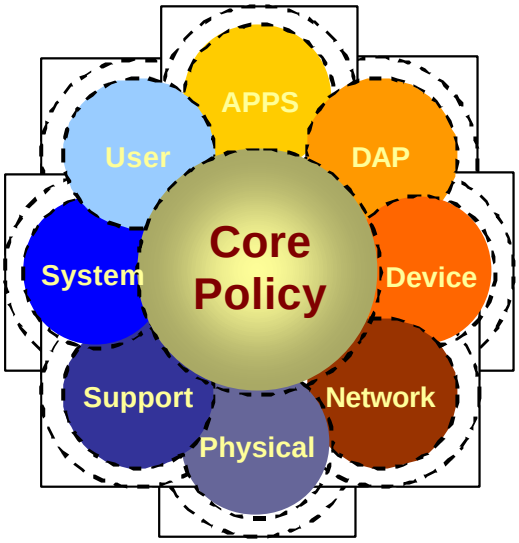


Figura 2.21 – Esquema do CIMv4.

O modelo de informação CIM é um componente de importância vital para o WBEM e outras tecnologias semelhantes, encontrando-se subdividido em três sub-modelos: o *core model* que reúne as características e noções aplicadas a todas as áreas da gestão, o *common model* que reúne as noções aplicáveis a determinadas áreas da gestão mas que são independentes da tecnologia ou da implementação e, finalmente, os *extension schemas* que representam objectos dependentes da tecnologia ou das implementações efectuadas.

Em termos de implementação, a Microsoft, que começou por desenvolver o WBEM antes deste passar para o DMTF, implementa nos seus sistemas uma tecnologia compatível com o WBEM, que dá pelo nome de *Windows Management Intrumentation* (WMI) com a arquitectura representada na Figura 2.22. Esta tecnologia já se encontra integrada nos sistemas Windows 98 e Windows 2000. A instrumentação no Windows NT 4.0 e Windows 95 pode ser feita mediante uma actualização do sistema.

Os vários componentes que constituem o WMI são descritos de seguida:

Gestor de Objectos CIM – entidade responsável pela manipulação da informação da base de dados CIM, onde reside a informação de gestão. Este processo não é responsável pelo acesso directo à informação de gestão, mas apenas providencia as funcionalidades CIM no acesso à informação.

Fornecedores de Serviços WMI – São os processos intermediários entre o Gestor de Objectos CIM e os componentes geridos. Quando o gestor de objectos CIM recebe um pedido de informação por parte da aplicação gestora, e não possui a informação na sua base de dados, redirecciona os pedidos para os fornecedores de serviços WMI. A Microsoft

no seu WMI SDK inclui fornecedores de serviços para o registo, o NT Event Log, o Kernel Win32, os componentes SNMP e os drivers WDM.

Segurança WMI – a segurança implementada pelo WMI é ainda reduzida, permitindo apenas o controlo de acesso de um utilizador à estrutura CIM. Em futuras realizações do WMI pretende-se estender esta funcionalidade às classes individuais.

Tratamento de Eventos – o processo de notificação é originado no elemento gerido e depois é encaminhado para a aplicação de gestão do mesmo modo que a restante informação.

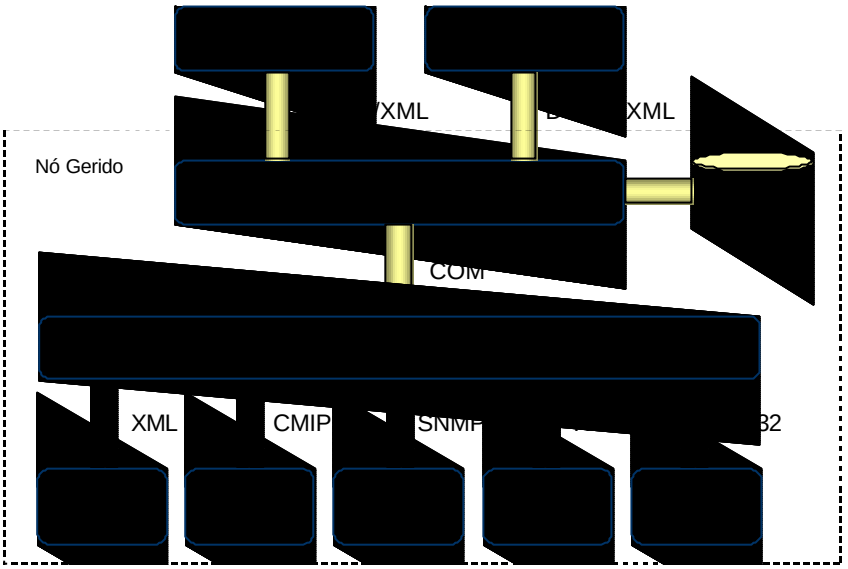


Figura 2.22 – Arquitectura do WMI.

É de referir ainda que o acesso à informação CIM, através do gestor de objectos CIM, pode ser feita também por um driver ODBC, possibilitando o desenvolvimento de aplicações que acedam à informação através deste driver [DMA00]. O WMI serve, actualmente, como infra-estrutura de base à maioria das aplicações de gestão da Microsoft (SMS, *Active Directory*, *Event Viewer*, etc.)

No contexto do CIM, surgiu ainda o *Directory Enabled Networks* (DEN), uma iniciativa conjunta da Microsoft e da Cisco que foi proposta ao DMTF em 1997. O DEN propõe-se definir um serviço de directoria que permita, automaticamente e num ambiente distribuído, associar aos utilizadores um conjunto de perfis, aplicações e políticas pré-definidas [RCW00].

O DEN tem como objectivos principais a constituição de um modelo e de um esquema que descreva todos os elementos necessários à configuração e gestão extremo a extremo de equipamentos e serviços, em função do utilizador, da aplicação e do serviço, potenciando uma maior integração da gestão das infra-estruturas TI no fornecimento de qualidade de serviços [WBU00]. O DEN faz o mapeamento do modelo CIM, que é um modelo

abstracto, numa estrutura de directório LDAP (Figura 2.23) onde serão armazenados os objectos, inter-relações e políticas da infra-estrutura [JHI00].

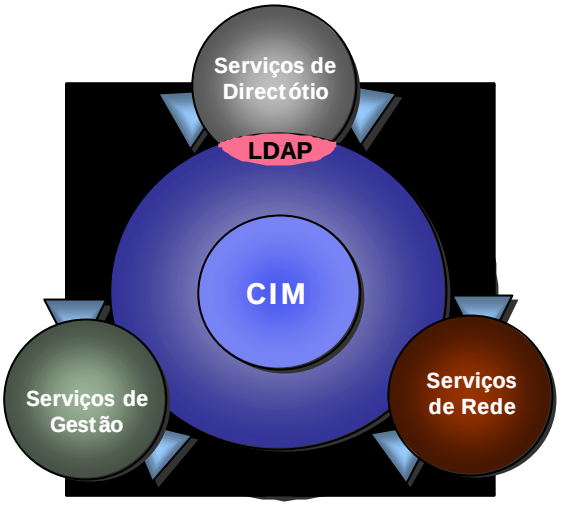


Figura 2.23 – Modelo de Informação do DEN (baseado em [RCW00]).

A implementação da filosofia associada ao DEN nos equipamentos de rede, nos serviços e nas aplicações potenciará a criação de infra-estruturas de informática inteligentes que, através da configuração num único ponto, os seus componentes automaticamente se reconfigurem de modo a responder às solicitações de serviço efectuadas (Figura 2.24).

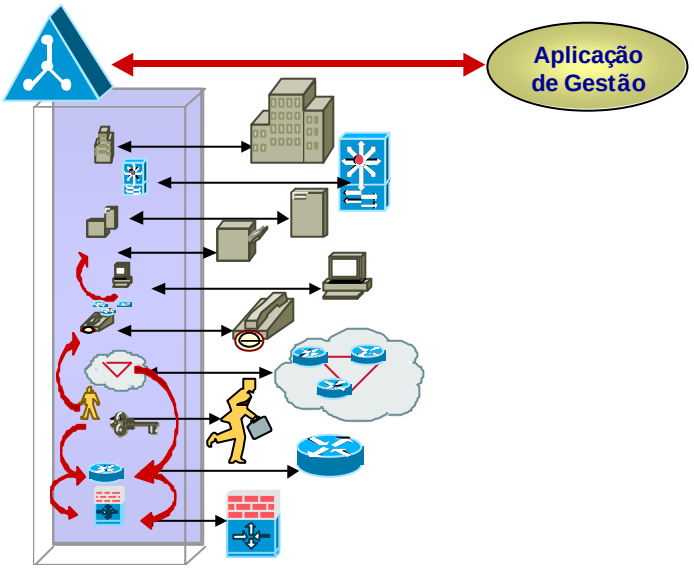


Figura 2.24 – Uma estrutura LDAP com os objectos geridos (baseado em [RCW00]).

3 Plataformas de Gestão

3.1 Introdução

O mercado das plataformas e aplicações de gestão é um mercado que sofreu uma grande evolução nos últimos anos assistindo-se a uma competitividade muito grande, que se faz a par com a evolução das tecnologias e infra-estruturas TI.

As soluções existentes no mercado são as mais variadas, estando dirigidas para todas as áreas da gestão. Recentemente as plataformas de gestão de redes têm perdido algum protagonismo para as plataformas de gestão de sistemas, acompanhando o papel fundamental que estes últimos têm assumido nas sociedades actuais. Segundo um estudo da *International Data Corporation* (IDC), actualmente, o investimento nas tecnologias de gestão de sistemas é já superior ao das tecnologias de gestão de redes, com crescimentos previstos de 13,2% e 7,7% até 2003, respectivamente [IDC00a]. Segundo a mesma fonte, a gestão de desempenho e a gestão de serviços, por esta ordem, passarão a dominar as atenções no mercado da gestão nos próximos dois anos.

A área da gestão, que tem assumido um papel cada vez mais importante, já tem no mercado, para além das aplicações de gestão, fornecedores de serviços de gestão (*Management Service Providers* – MSPs) [ASH00a]. Este novo fornecedor de serviços é uma solução adequada para as empresas que não queiram investir em conhecimento, soluções e recursos humanos, delegando as tarefas de monitorização, configuração e análise numa empresa externa e focando-se apenas na sua área de negócio [MMSM00].

Um estudo prévio do mercado será fundamental para, de entre toda a panóplia de aplicações, comerciais e de domínio público, identificar as que melhor se enquadram nas necessidades específicas de cada caso e implementem as normas de gestão actuais, normas que, em muitos casos, não passam de mera propaganda e "chavões" das empresas [BGO99].

Neste capítulo serão apresentados os requisitos de um sistema de gestão e, face a esses requisitos, será efectuado um estudo de mercado, com o objectivo de identificar várias aplicações comerciais e de domínio público, analisando-as e testando-as para que sobressaiam as qualidades e deficiências de cada solução. Este estudo será complementado com análises e estudos efectuados por entidades da área [NWF01a].

Depois de identificadas as aplicações a usar, será feita uma descrição, mais pormenorizada dessas aplicações tendo em conta o modo como podem ser integradas.

3.2 Requisitos de Uma Plataforma de Gestão

A constituição de uma plataforma de gestão que responda às necessidades de gestão de redes e sistemas deverá ser pautada pelo estabelecimento de um conjunto de requisitos, que se adeqúem às necessidades de gestão actuais de uma infra-estrutura informática.

Seguindo esta perspectiva, será elaborado um "caderno de encargos" sobre soluções de gestão, que será a base de trabalho para o estudo de mercado a realizar, nomeadamente tendo em conta factores como o preço, funcionalidades, estratégias de desenvolvimento, entre outros, que melhor se adeqúem às funções pretendidas. Neste quadro será dada importância à análise de factores como:

- Descoberta automática da topologia da infra-estrutura;
- Monitorização permanente dos objectos e sincronismo dos mapas de rede;
- Tratamento de eventos;
- Escalabilidade;
- Monitorização de serviços;
- Integração com outras aplicações;
- Suporte de SNMP, RMON e RMON2;
- Suporte de DMI, CIM/WBEM, DEN;
- Configuração remota de equipamentos;
- Distribuição de software;
- Controlo remoto de sistemas;
- Inventário de software e hardware;
- Controlo de licenças de software;
- Disponibilização de mecanismos de exportação de dados para bases de dados relacionais, por exemplo SQL;
- Disponibilização de interface Web, para acesso à informação e funções de gestão;
- Custo;
- Serviço de suporte prestado pelo fabricante;
- Aceitação e quota de mercado;
- Desempenho;
- Facilidade de operação;
- Implementação de políticas de gestão;

3.3 Plataformas de Gestão Generalistas

3.3.1 Solstice Site Manager / Solstice Domain Manager

Uma das empresas mais conceituadas no mercado, a SUN, apresenta nesta área a plataforma Solestice. O Solestice resulta de uma evolução da plataforma de gestão da SUN, integrada com uma tecnologia proprietária *Cooperative Consoles* [SUN00c], sendo a

sucessora do *SunNet Manager*, que constituía, até há pouco tempo, a única plataforma disponibilizada por esta empresa. O *Solestice* apresenta-se em duas versões distintas, dirigidas a diferentes nichos de mercado e utilizando o SNMP, como protocolo de comunicação com os equipamentos. A primeira, o *Solestice Site Manager* (SSM), é indicada para redes de pequena dimensão, até 100 nós, e a segunda, o *Solestice Domain Manager* (SDM), foi concebida para suportar redes de grande dimensão e desempenhar funções de gestão em WANs [SUN00b].

O *Solestice* funciona apenas em ambientes *Solaris* o que, para o presente cenário de implementação, é uma desvantagem, no que diz respeito aos ambientes suportados e aos custos envolvidos. No entanto, é uma plataforma que em termos de distribuição e escalabilidade tem já méritos reconhecidos. Podendo funcionar como estação única ou em conjunção com outras estações, permitindo a troca de informação e distribuição das funções de gestão, potencia uma plataforma distribuída e escalável.

O *Solestice* apresenta uma característica deveras interessante, que é a possibilidade de distribuir agentes, os *Mid-Level Managers*, pela infra-estrutura, delegando neles a recolha de informação estatística, reduzindo o tráfego de gestão na rede e possibilitando a interacção com outros objectos que, por utilizarem outros protocolos, não são directamente geríveis pelo *Solestice* o qual, relembrando, funciona apenas em ambientes *Solaris* utilizando TCP/IP.

No que respeita à integração com outras plataformas, o *Solestice* apresenta um leque bastante reduzido de opções, quando comparado com outras aplicações do mesmo género.

3.3.2 IBM Tivoli NetView

O *NetView* é um produto da Tivoli, empresa que foi fundada por funcionários da IBM e, posteriormente, adquirida por esta, assumindo um papel importante no mercado das soluções de gestão de redes e sistemas.

O *Tivoli*, e o seu vasto leque de aplicações, apresentam-se como uma solução integrada que pretende dar resposta a todas as áreas da gestão. Na presente descrição vamo-nos focar apenas numa aplicação específica, o *NetView*, que, podendo funcionar em ambientes Unix ou Windows, apresenta-se como uma plataforma escalável e com um conjunto de funcionalidades que a tornam, actualmente, uma das líderes de mercado na área da monitorização de redes.

O *NetView* para além de todas as funções de descoberta automática de rede, monitorização, recolha de estatísticas, recepção e análise de eventos, isolamento de problemas, implementa gestão baseada em políticas pré-definidas. Esta funcionalidade é interessante na medida em que podem ser definidos contentores de objectos, para os quais é definido um conjunto de políticas (Ex: recolha de estatísticas de determinadas variáveis, acções a tomar mediante a recepção de eventos, encaminhamento de alertas, ...). Sempre que um

novo objecto seja adicionado a esse contentor, herda as propriedades referidas, o que potencia um modo simples e rápido de configuração de novos objectos.

Em termos de escalabilidade e distribuição, o *NetView*, permite a coexistência e inter-relação entre várias estações de gestão, auxiliadas nas suas funções, por agentes *Mid-Level Managers* que desempenharão funções de gestão para os objectos da sub-rede onde se encontram. A integração com outras aplicações é também um dos pontos-chave do *NetView*, existindo um conjunto de várias dezenas de fabricantes cujas aplicações se integram com esta plataforma. No entanto esta integração, sem problemas para as restantes aplicações da Tivoli, apresenta-se com algumas dificuldades de implementação quando estão envolvidas aplicações de terceiros, essencialmente, no que diz respeito a questões técnicas, não sendo triviais os procedimentos de integração [SEL99].

3.3.3 Cabletron Spectrum

A Cabletron Systems dividiu-se em quatro empresas distintas para dar melhor resposta às várias áreas de negócio das infra-estruturas TI. As questões relativas à gestão são endereçadas pela Aprisma. Assim, o *Cabletron Spectrum* da Aprisma é mais uma das aplicações a competir pela quota de mercado na área das plataformas de gestão de redes e é, segundo algumas análises, uma das aplicações com maiores potencialidades, essencialmente, pela sua escalabilidade e integração. No que respeita às funcionalidades, o *Spectrum*, situa-se muito próximo dos concorrentes, implementando mecanismos de descoberta automática da rede, isolamento de problemas, recolha de estatísticas, armazenamento de dados em formatos normalizados (SQL), tendo sido mesmo considerado como o primeiro na gestão de alarmes [SEL99]. O acesso à estação de gestão foi também cuidado, disponibilizando uma interface WEB, o que permite o acesso à informação de gestão em qualquer altura em qualquer lugar, já que o uso dos browsers WEB se encontra generalizado.

Em ambientes Unix e Windows e sem aplicações adicionais, o Spectrum suporta a gestão de mais de 500 equipamentos de rede de diversos fabricantes, o que constitui uma importante mais valia, uma vez que elimina a necessidade de adquirir aplicações específicas, de cada fabricante, para efectuar as operações básicas de gestão sobre os seus equipamentos, apresentando como manifesta vantagem a redução dos custos totais da plataforma.

3.3.4 HP OpenView NNM

A Hewllet Packard possui uma das mais vastas gamas de produtos relacionados com gestão, quer de redes, quer de sistemas e serviços, com soluções que abordam todos os níveis do modelo OSI e todas as áreas funcionais da gestão [AWI01]. Dessa panóplia de produtos, o *Network Node Manager* (NNM) da família *OpenView*, é a plataforma mais divulgada e utilizada no contexto de gestão lógica de redes, descobrindo, identificando e disponibilizando mapas da configuração lógica da rede (Figura 3.1) sobre os quais é

possível efectuar um conjunto de operações de gestão. Esta plataforma foi, e continua a ser, desenvolvida para várias configurações de hardware (HP, SUN, Intel, …), e também para funcionar na maioria dos ambientes de sistema operativo (HP-UX, SUN OS, Solaris, Windows NT).

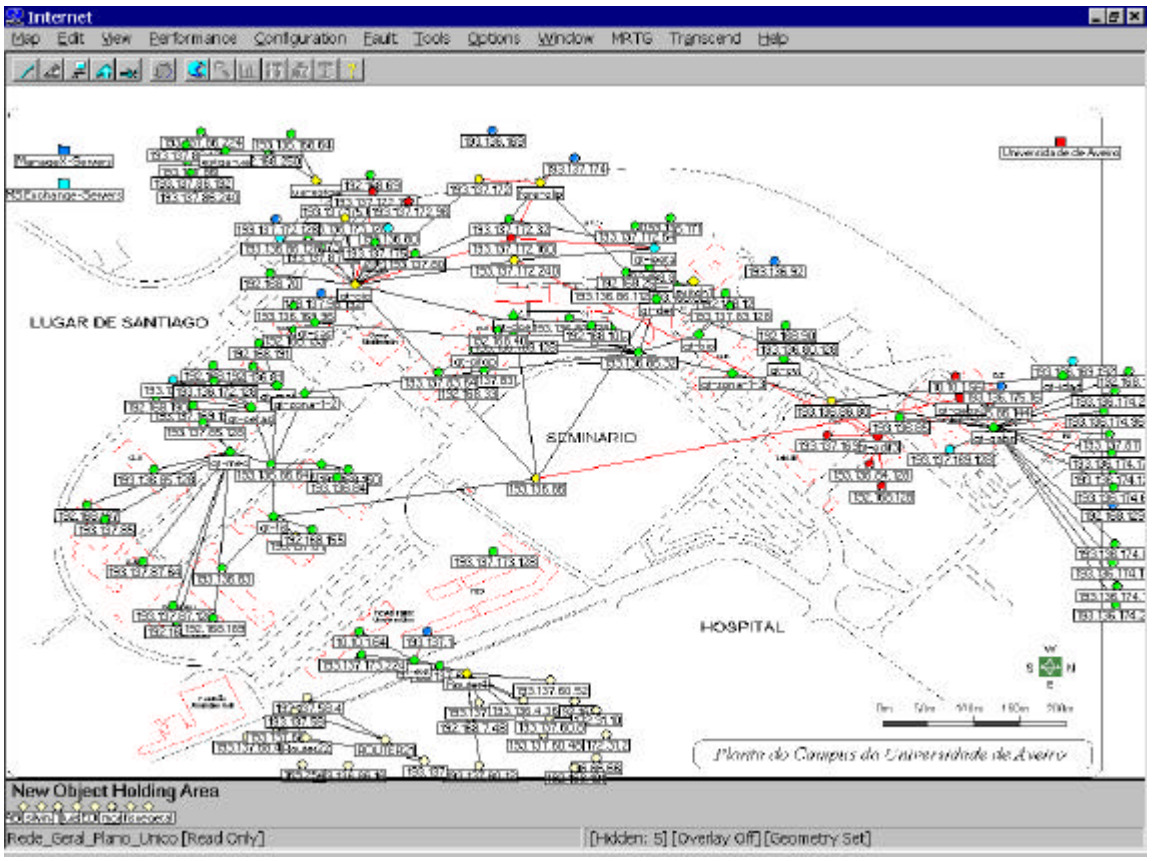


Figura 3.1 – Apresentação gráfica do NNM.

A liderança no mercado da gestão e um reconhecimento merecido ao longo de vários anos de domínio de mercado, fazem do NNM e da família *OpenView* uma das soluções melhor constituídas e com mais crédito na área da gestão.

Desde sempre, foi objecto da política de integração do NNM a parceria com outros fabricantes, de modo a desenvolver as aplicações de gestão de equipamentos específicos a serem integradas com o NNM. Actualmente contam-se cerca de 200 fabricantes cujas aplicações de gestão se podem integrar com o NNM [HPOV00b].

Uma outra aposta por parte da HP, comum a outras empresas da mesma área, é a disponibilização de um interface WEB para as suas aplicações de gestão. A partir da versão 6.0, o NNM passa a incluir uma interface WEB baseada em JAVA, o que possibilita o acesso a partir de qualquer ponto da rede à aplicação de gestão.

O acesso à informação é sempre um factor muito importante a ter em conta nas aplicações de gestão. Quando a gestão pode ser distribuída por mais de uma estação, um elemento

essencial na plataforma de gestão é a existência de um repositório central onde possam ser armazenados os dados. No NNM este "depósito" pode ser baseado numa base de dados Oracle [GKO95] ou SQL [CJD97].

Muitas vezes, as soluções existentes no mercado não respondem inteiramente a todas as necessidades dos gestores. Existe sempre esta ou aquela particularidade da infra-estrutura que a plataforma adquirida não suporta. A pensar nestas questões, a HP disponibiliza o NNM *Developer Toolkit*, que não é mais que um conjunto de APIs para efectuar o desenvolvimento (em C ou C++) de aplicações que visem satisfazer cada necessidade para a qual a plataforma não tem capacidade de resposta directa.

3.3.5 Unicenter TNG

O *Unicenter TNG* da Computer Associates International (CAI) é mais do que uma aplicação de gestão de redes e sistemas. A CAI propõe-se oferecer com este produto uma única plataforma integrada que possibilite a gestão completa dos equipamentos e dos sistemas e serviços. Nesta perspectiva o Unicenter TNG fornece um conjunto de interfaces que permitem modelar a visualização da rede de acordo com a realidade, inclusive numa perspectiva tridimensional.

O *Unicenter TNG* baseia o seu funcionamento na constituição de uma *framework* proprietária, implementada à custa de agentes próprios instalados por todos os sistemas da infra-estrutura, que disponibiliza toda a informação e funcionalidades a usar pela aplicação de gestão.

Na área da gestão de rede, e em termos de funcionalidades, a aplicação é muito semelhante às já referidas sendo de destacar a flexibilidade e escalabilidade proporcionadas por uma filosofia cliente/servidor, que possibilita que mesmo os equipamentos que não possuam as características de gestão normais (SNMP) possam ser geridos de uma forma integrada através de agentes que se instalam nesses equipamentos. A pensar na coexistência de aplicações e no aproveitamento de tecnologias, o *Unicenter TNG* inclui ferramentas que suportam uma grande variedade de sistemas como o Windows, UNIX, VMS, OS/400, etc.

Na área da gestão de sistemas, o *Unicenter TNG* permite efectuar, entre outros, o inventário de hardware e software, a distribuição de software e o controlo remoto do sistema, estando dotado de uma série de agentes para os mais variados sistemas operativos (Windows 9x/NT/2000, Unix, Linux, OpenVMS, NetWare, OS/400,...). Nesta área comporta-se de forma idêntica ao *Systems Management Server* (SMS) da Microsoft, apresentando a vantagem de integrar todas estas funcionalidades com as restantes funções de gestão da infra-estrutura.

Em termos de integração com terceiros, o *Unicenter TNG* apostou em parcerias com cerca de uma dúzia de empresas estratégicas, passando a incluir um leque alargado de opções e funcionalidades que fazem dele uma solução integrada para a gestão completa de todo o ambiente de informática da empresa.

3.3.6 *Microsoft Systems Management Server*

A Microsoft, com a sua plataforma de gestão o *Systems Management Server* (SMS) cuja consola é apresentada na Figura 3.2, é uma das empresas que está há mais tempo no mercado com soluções abrangentes na área da gestão de sistemas, acompanhando a evolução dos sistemas da Microsoft e beneficiando do conhecimento profundo da implementação desses mesmos sistemas [NWI00].

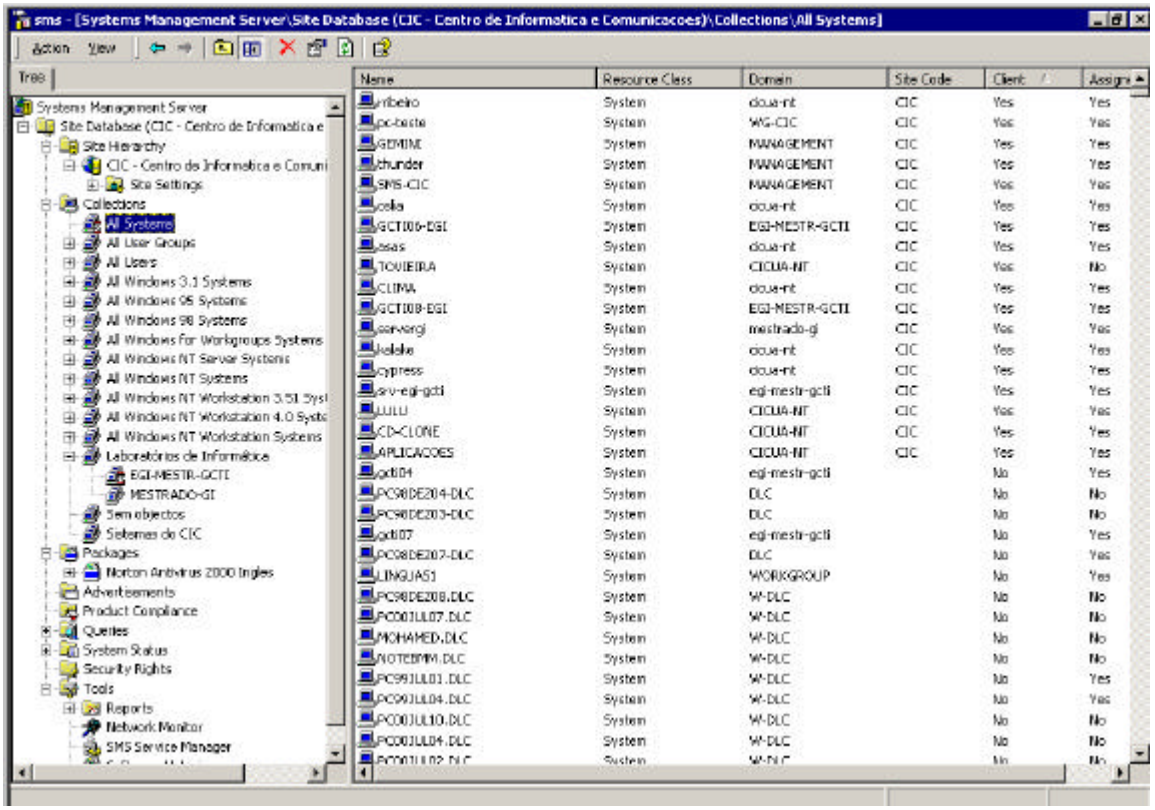


Figura 3.2 – Consola do SMS.

O SMS, que está neste momento na versão 2.0, apresenta evidentes aperfeiçoamentos comparativamente à sua anterior versão e as suas funcionalidades harmonizam com as normas de gestão de sistemas em uso actualmente. Aliás, diga-se que a Microsoft tem sido um dos principais impulsionadores das iniciativas do DMTF [DMTF01a].

Em questões de funcionalidades e facilidade de operação, o SMS está na linha da frente em termos de posicionamento no mercado, apresentando um preço competitivo com outras soluções do mercado. Ainda relativamente ao preço, e dadas as políticas de licenciamento da Microsoft, as instituições de ensino usufruem de condições que dificilmente serão batidas pela concorrência [TCO00a].

O SMS apresenta boas características de escalabilidade, funcionando sobre o Windows NT/2000 e podendo utilizar como pontos de distribuição sistemas Novell Netware e

suportando apenas clientes Microsoft. Nas funcionalidades destacam-se o inventário de hardware e software, a distribuição de software, o controlo remoto de sistemas, o controlo da largura de banda ocupada pelas operações de gestão e manutenção e um conjunto de configurações que fornecem uma granularidade muito elevada no controlo de todo o sistema.

Do lado dos sistemas operativos, o Windows 2000 aparece como a primeira família de sistemas operativos pensada para fazer uso, do que há de mais recente nos conceitos e nas tecnologias de gestão de sistemas e de redes, reflectindo-se na redução dos custos de manutenção [CRN01]. No âmbito da gestão de redes é de destacar, para além do que já existia disponível para as anteriores versões, a implementação da *host-resources-mib* [RFC1514], que disponibiliza um conjunto de informação muito valiosa. Já na gestão de sistemas o Windows 2000 evidencia-se pelo suporte nativo do WMI, que é a base de funcionamento de várias das aplicações de gestão e monitorização de recursos do sistema [MSC00d]. Para além do WBEM são também implementados conceitos da iniciativa DEN, através da *Active Directory*, onde são armazenados todos os objectos da infra-estrutura e políticas a aplicar-lhes, que definirão o seu comportamento, enquanto elementos constituintes do sistema [MSC00b].

A Tabela 3.1 é ilustrativa de uma série de funcionalidades, que passam pelo suporte à mobilidade dos utilizadores com os perfis remotos, as pastas off-line e o redireccionamento de pastas, incluindo mecanismos para instalação de software com o *Remote Instalation Service* (RIS), o *Windows Installer* [MSC99d] e o suporte de DHCP, incluindo a definição de políticas de utilização dos recursos como as quotas de disco.

Tabela 3.1 – Funcionalidades suportados pelos sistemas Windows 2000.

Área		Funcionalidades e tecnologias
Intelli Mirror	Gestão de dados dos utilizadores	✍ Active Directory ✍ Group Policy ✍ Offline Folders ✍ Synchronization Manager ✍ Disk Quotas.
	Manutenção e instalação de software	✍ Active Directory ✍ Group Policy ✍ Windows installer service
	Gestão de utilizadores e políticas	✍ Active Directory ✍ Group Policy ✍ Offline Folders ✍ Roaming User Profiles
Instalação remota de sistemas		✍ Active Directory ✍ Domain Name System (DNS) ✍ Dynamic Host Configuration Protocol (DHCP) ✍ Remote Installation Server

Os mecanismos de gestão disponibilizados pelo Windows 2000 fazem uso, na sua maioria, das facilidades disponibilizadas pelo WMI, sendo fornecido um conjunto de scripts e APIs

[MSC00c], que facilitam a programação de aplicações adaptando-as a necessidades específicas.

O SMS tira o maior partido das funcionalidades referidas e do facto de ser propriedade do mesmo fabricante, colocando-se numa posição de destaque no domínio do mercado das plataformas de gestão de sistemas.

3.3.7 Intel LANDesk Management Suite

A Intel possui uma das plataformas de gestão de sistemas mais cotadas do mercado, o *Intel LANDesk Management Suite.* Esta plataforma fornece, por um preço competitivo, um conjunto de funcionalidades que vão desde inventário de software e hardware, passando por funções específicas e diferenciadas para a gestão de servidores e clientes, distribuição de software, protecção antivírus dos clientes, até a disponibilização de uma interface Web. A escalabilidade é talvez um dos seus maiores méritos adaptando-se quer a redes de pequena dimensão quer a redes de grande dimensão, funcionando sobre vários sistemas (Windows, Netware, Linux,...) e suportando uma multiplicidade de clientes de várias famílias de sistemas operativos [TCO00a].

O *LANDesk* oferece compatibilidade e implementa as mais recentes tecnologias de gestão de sistemas, apenas não integrando ainda os conceitos do DEN. No que se refere ao armazenamento e trato dos dados é disponibilizada a integração com várias bases de dados, acessíveis por ferramentas que fornecem uma conjunto de estatísticas e relatórios sobre a infra-estrutura.

A gestão centralizada de licenças e distribuição de software admite um controlo e optimização efectivos do software e licenciamento da organização, bem como, providencia mecanismos de actualização remota e fora de horas, dos sistemas clientes.

3.3.8 Spectrum Enterprise Manager e Metrix WinWatch

Dadas as suas parcerias estratégicas a Aprisma consegue, tendo por base o *Cabletron Spectrum*, constituir uma plataforma integrada de gestão de redes e sistemas. Esta mais valia é conseguida com o *Metrix WinWatch*, aplicação desenvolvida pela Metrix. Estas duas aplicações integradas conseguem reunir um conjunto de funcionalidades invejável abarcando praticamente todas as questões relacionadas com a gestão aos vários níveis OSI. As funções enumeradas, como sendo suportadas por esta plataforma, são todas a referidas até aqui, com a excepção do suporte, claro, da norma CIM/WBEM. No entanto, esta integração tem um preço muito elevado, talvez demasiado alto para ser uma solução competitiva, reflectindo-se numa desvantagem da solução.

3.4 Aplicações de Gestão Específicas

As plataformas base podem ser complementadas com aplicações de terceiros (*Third-parties*) que normalmente estendem as capacidades de gestão dessas plataformas. Sendo a panóplia de aplicações muito vasta, nesta secção serão abordadas apenas algumas que estarão de acordo com as necessidades de gestão existentes na infra-estrutura onde se pretende implementar a plataforma de gestão.

3.4.1 Transcend Enterprise Manager

A 3COM possui uma aplicação o *Transcend Enterprise Manager* (TEM), com uma série de funcionalidades que permitem facilmente tirar partido de todas as potencialidades dos equipamentos da marca, encontrando-se entre as melhores posicionadas no mercado em termos de mecanismos de gestão disponibilizados pelos equipamentos [ERP99].

Entre outras características, o TEM disponibiliza mecanismos de configuração e actualização automática de equipamentos tendo por base: configurações e políticas definidas pelo gestor, a visualização física dos equipamentos que possibilita uma dimensão física para além da dimensão lógica, a alteração de configurações através de uma interface gráfica e a monitorização de variáveis relativas ao tráfego e às condições da rede.

Esta aplicação permite ser integrada com o NNM conjugando as potencialidades das duas aplicações numa mesma interface. Na versão correntemente em análise, o TEM97, existe uma deficiência que poderá eventualmente ser resolvida e que se relaciona com o facto do TEM necessitar de uma base de dados própria (em *Sybase SQL Anywhere*), quando poderia utilizar a base de dados do NNM sem ser necessário duplicar a informação.

3.4.2 Marconi ServiceOn Foundation

A Fore, uma das empresas líderes no mercado da tecnologia ATM, foi recentemente adquirida pela Marconi, em conjunto com todos os seus produtos. O *ForeView*, aplicação da Fore que permitia a gestão dos equipamentos através de uma interface gráfica guiada visualmente, está agora integrado com *ServiceOn Foundation* que já era um produto da Marconi. Esta aplicação encontra-se vocacionada para a gestão dos serviços da Marconi englobando a gestão de rede ATM e IP no que respeita à topologia, falhas, configuração e desempenho, sendo mais abrangente que o *ForeView* que apenas se dedicava à gestão dos equipamentos Fore.

Em termos de características, para além de poder ser integrado com o NNM, pode funcionar sobre sistemas Windows NT/2000 ou Solaris e apresenta um conjunto de funcionalidades que, por si só, fazem o sistema funcionar de modo autónomo. Esta autonomia é garantida por um sistema de eventos próprio de descoberta e actualização dos mapas de rede e estado dos objectos, pela adaptação a produtos de outros fabricantes, pela

escalabilidade, pela interface amigável e pela integração com bases de dados externas [MAR00].

Em termos específicos, a aplicação permite a gestão de perfis, de SVCs e PVCs através de assistentes e escalonados temporalmente, a identificação de percursos, a abertura de aplicações contextualizadas com os equipamentos e o acesso via Web através de HTML e JAVA.

Esta aplicação apresenta grandes vantagens na gestão de redes de grande dimensão interligadas por equipamentos ATM e redes de fornecedores de serviços que, à semelhança da Marconi, alugam aos seus utilizadores circuitos do mais variado tipo, usufruindo das funcionalidades de gestão oferecidas nesta área.

3.4.3 CiscoWorks

A Cisco, líder no mercado nos equipamentos de encaminhamento em redes IP, desenvolveu a aplicação *CiscoWorks*, disponibilizando uma interface de configuração gráfica guiada visualmente para os seus equipamentos. O *CiscoWorks* facilita as tarefas de configuração e gestão dos equipamentos eliminando, quase na totalidade, a necessidade de utilizar a linha de comandos.

O *CiscoWorks*, actualmente na versão 2000, está dividido em três componentes: o *LAN Management Solution*, o *Routed WAN Management Solution* e o *Service Management Solution*. Estes podem funcionar individualmente, em conjunto ou integrados com outras plataformas de gestão, por exemplo o NNM. Cada um dos componentes tem atribuído funções distintas correspondendo a níveis de gestão diferentes, sendo a disponibilização de uma interface Web para todas as suas funções uma característica presente em todas elas [CIS00].

O *LAN Management Solution* está vocacionado para a gestão de uma infra-estrutura local de comunicações, baseada em comutadores de nível 2 e 3, através de um conjunto de ferramentas para configuração, monitorização, análise e detecção de falhas nesses equipamentos, destacando-se por exemplo o *CiscoView* (Figura 3.3).

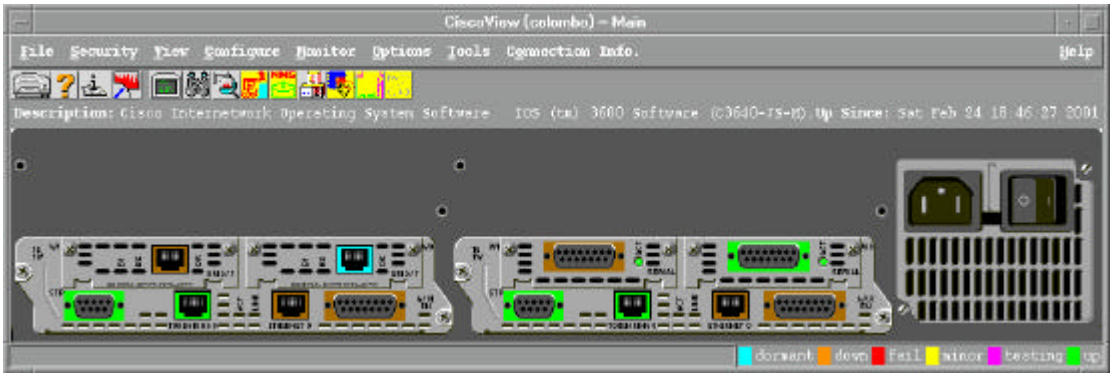


Figura 3.3 – Interface do CiscoView.

O *Routed WAN Management Solution* apresenta-se vocacionado para a gestão de infra-estruturas de rede de área alargada baseada em encaminhadores, disponibilizando ferramentas para a gestão de múltiplos serviços sobre a mesma infra-estrutura.

O *Service Management Solution* é uma solução para a gestão de qualidade de serviço fornecida por uma infra-estrutura de comunicações.

O CiscoWorks é uma aplicação baseada nas normas de gestão em vigor, tendo como grandes pontos a seu favor a integração com outras aplicações, a disponibilização de um conjunto muito completo de ferramentas para gestão dos equipamentos Cisco, sendo particularmente interessante na gestão de uma infra-estrutura que pretenda fornecer vários serviços com diferente qualidade, qualidade esta baseada em perfis de utilizadores ou de aplicações.

3.5 Outras Aplicações

As facilidades disponibilizadas pelos agentes RMON e RMON2 nomeadamente na análise de tráfego e desempenho ao nível das várias camadas protocolares estão a generalizar a sua utilização nos equipamentos de rede [PMO00]. Os dados recolhidos por estes agentes distribuídos pela rede, são tratados por aplicações desenvolvidas para efeito e que possibilitam uma análise visual dos eventuais problemas ou apenas a evolução de tráfego num determinado segmento.

Nesta área, tal como acontece em todas as áreas da informática, a concorrência é muita e as aplicações existentes são inúmeras, existindo sempre algumas que, quer pelas suas funcionalidades, quer pela facilidade de utilização, se destacam no mercado.

Entre as aplicações de gestão RMON, encontram-se o *NetMetrix* da HP, o *Traffix Manager* da 3COM, o *Observer* da Network Instruments e uma série de outras que foram alvos de estudos de mercado [NWC00a]. Estas aplicações disponibilizam ao utilizador uma interface gráfica onde podem ser analisados dados relativos ao comportamento de um troço de rede, à comunicação estabelecida entre quaisquer máquinas desse troço, os protocolos e aplicações mais utilizados. Dados os custos envolvidos, para o presente trabalho, será apenas estudado o *Observer Suite.*

A aplicação *Observer Suite* possibilita mais do que a análise dos dados coleccionados pelas sondas RMON, podendo funcionar numa arquitectura cliente/servidor onde o cliente é uma sonda proprietária que estende as capacidades dos agentes RMON. Esta aplicação funciona em qualquer sistema Windows 9x/NT e fornece uma série de funcionalidades, entre elas a disponibilização de sondas em software, a análise dos tempos de resposta dos vários sistemas e a disponibilização dos dados através de uma interface Web. Entre as maiores vantagens desta aplicação observamos um vasto leque de funcionalidades e o seu baixo preço. Em contrapartida as maiores desvantagens são a instabilidade manifestada pela aplicação quando efectua a monitorização simultânea de várias variáveis e a falta de integração com outras aplicações, como revelou o estudo da aplicação.

A análise de tráfego em tempo real de um troço de rede pode ser efectuada por software que faz essa monitorização e apresenta os resultados ao gestor na própria consola. Esta aproximação tem desvantagens que se relacionam essencialmente com a necessidade de deslocação do gestor ao local de monitorização, mas por outro lado, apresenta vantagens significativas relativamente aos custos do software de monitorização. As características referidas podem encontrar-se em diversas aplicações, entre elas o *Sniffer Pro*, o *NetxRay* e o *Agilent Advisor*.

A maioria das aplicações referidas anteriormente contempla apenas a monitorização dos troços de rede e disponibilidade dos sistemas, deixando de parte os serviços que aqueles têm implementados. O *BigBrother* [BBR00] é uma aplicação baseada numa filosofia cliente servidor cuja principal função é monitorizar serviços e sistemas. Entre as suas funcionalidades encontra-se uma interface Web para o acesso à informação, sendo capaz de receber e tratar notificações através de um sistema de alertas e inclui um sistema de tratamento de dados com geração de relatórios que permite, em qualquer altura, ter a informação do comportamento dos sistemas ao longo tempo. Esta aplicação vem já com um sistema de redundância implementado, permitindo a sua instalação em vários servidores que depois interagem entre si. A aplicação tem funcionalidades bastante interessantes apresentando como principal desvantagem a falta de integração com outras aplicações.

Para terminar esta descrição fica aqui uma outra aplicação que não está vocacionada propriamente para a gestão de redes, mas antes para o registo de cadastro físico da infra-estrutura, o *IT Layers*, da Hytachi Software Engineering América. O *IT Layers* é um software semelhante a um sistema de informação geográfica (SIG) que permite a criação dos mapas da rede com base na informação retirada do NNM ou do SMS, por exemplo, dispondo-a em consonância com a localização física dos equipamentos (Figura 3.4). Até aqui, as vantagens do sistema ficam-se pela integração com plataformas de gestão, mas as características que mais sobressaem são a possibilidade de com um simples clique, saber qual a distância real entre dois equipamentos, identificar o caminho físico entre dois sistemas, o acesso a toda a informação relevante sobre um sistema e o armazenamento da informação em bases de dados SQL. Analisando estas características do ponto de vista da manutenção, depois do sistema implementado, em poucos minutos consegue-se, por exemplo, fazer uma estimativa orçamental para a actualização da infra-estrutura e dos equipamentos. Uma aplicação deste género é com certeza um factor importante na competitividade das empresas, até porque permite, em qualquer momento, ter uma noção exacta do estado da infra-estrutura a todos os níveis.

As aplicações comerciais e as grandes plataformas de gestão nem sempre resolvem todas as situações e, muitas vezes, as necessidades de gestão não justificam o preço que se paga por uma plataforma comercial e integrada. As aplicações de domínio público são em alguns casos a solução (senão a ideal pelo menos a possível), existindo ferramentas que satisfazem quase todas as necessidades, mas sempre em pequenas peças que quase nunca

são integráveis sem programação adicional, mas que respondem às necessidades. De seguida serão descritas algumas destas ferramentas.

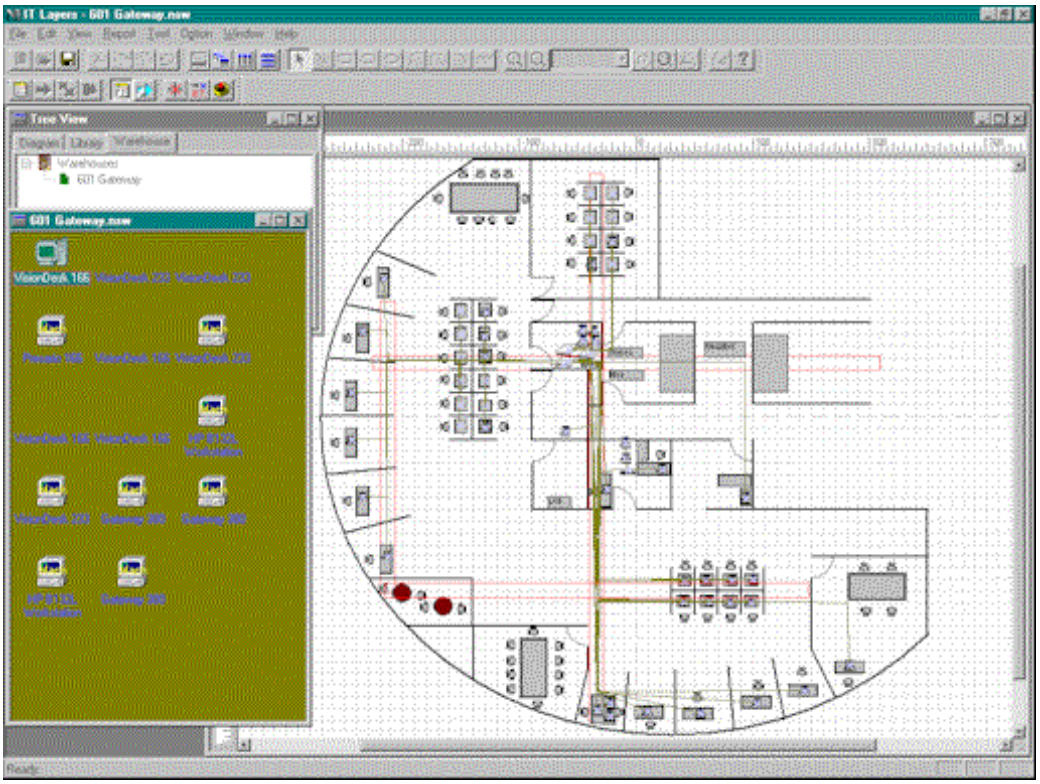


Figura 3.4 – Interface do IT Layers.

Na área da monitorização estatística, o *Multi Router Traffic Grapher* (MRTG) [TOE00], que surgiu em 1994 de uma necessidade específica, apresenta-se como uma solução muito eficiente e bastante utilizada para a monitorização de tráfego nas interfaces dos equipamentos. Programado em PERL e C, recolhe os dados gerando um gráfico semelhante ao da Figura 3.5.

Os dados são recolhidos e armazenados, permitindo ter uma estatística longitudinal do tráfego (diária, semanal, mensal e anual). O MRTG pode ser integrado com o OpenView NNM, disponibilizando assim os dados recolhidos pelo NNM numa interface WEB, permitindo o acesso aos mesmos de uma forma mais simples e versátil, do que a fornecida pelo NNM.

A conectividade dos sistemas não é necessariamente um indicador efectivo da disponibilidade dos serviços. O *NetSaint* é equivalente ao *BigBrother* e implementa mecanismos que possibilitam o teste de conectividade e dos serviços que possam estar implementados num equipamento. Esta aplicação, para além de possuir uma interface WEB bastante completa, pode também enviar alertas por correio electrónico ou pager. A configuração para além de permitir um conjunto muito vasto de possibilidades, podendo

efectuar-se através da interface WEB ou directamente nos ficheiros de texto que servem de configuração ao serviço NetSaint, apresenta-se algo complexa e de difícil execução.

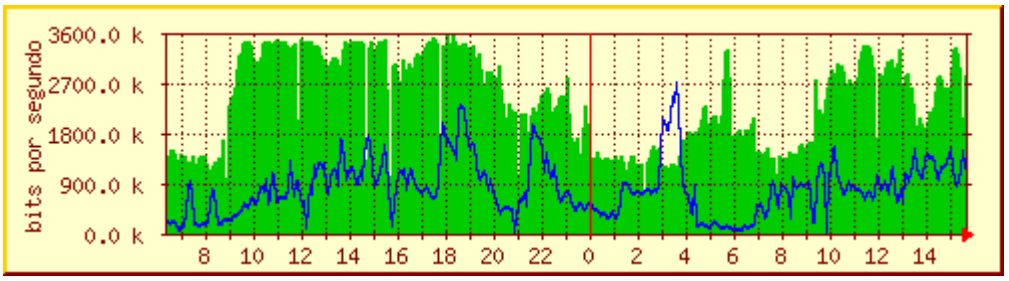


Figura 3.5 – Gráfico diário gerado pelo MRTG.

Na área da monitorização de tráfego é de bastante utilidade uma ferramenta de domínio público que permita a monitorização de tráfego num determinado segmento de rede, no que respeita à quantidade, tipo, origem e destino. O *IPTraf* é uma destas aplicações e apresenta uma característica que a maioria das aplicações comerciais não dispõe – monitoriza e enumera os portos que são utilizados na comunicação no troço de rede, independentemente de serem portos normalizados – normalmente, as aplicações juntam as estatísticas de todos os portos que não se encontram predefinidos e apresentam esses resultados como "outros". O *IPTraf* efectua a separação por portos (Tabela 3.2), sem haver a necessidade de recolher tráfego para posterior análise.

Tabela 3.2 – Informação recolhida pelo IPTraf.

Proto/Port	Pkts	Bytes	PktsTo	BytesTo	Pkts From	Bytes From
TCP/www:	10552336	6042000000	4880103	517320000	5672233	5525000000
TCP/8000:	1215637	954931000	484434	19710303	731203	935221000
TCP/ftp-data:	1089245	947230000	573851	478081000	515394	469149000
TCP/smtp:	1228932	890974000	740123	865766000	488809	25208516
TCP/6699:	910924	686271000	368300	58141349	542624	628130000
TCP/6688:	793763	654378000	303639	23181258	490124	631196000
TCP/nntp:	560272	418577000	316963	394796000	243309	23781579
UDP/domain:	616774	80759932	310303	39515221	306471	1244711
TCP/9216:	531430	73176674	265352	14209746	266078	58966928
TCP/https:	241738	69159009	127220	13604173	114518	55554836
TCP/imap2:	91053	58403350	40152	1878123	50901	56525227
TCP/pop-3:	141715	51600533	60005	2651005	81710	48949528
TCP/6700:	44797	36865084	18952	870623	25845	35994461
TCP/554:	43538	20386523	20387	1100558	23151	19285965
TCP/ircd:	161884	13516706	81213	3878754	80671	9637952
...	...	...	...	...	...	...

O GetIf é um utilitário que concentra numa mesma interface um conjunto de ferramentas de teste e diagnóstico de problemas em redes IP. Das ferramentas distinguem-se, entre outras, um MIB Browser, um traceroute, diagnóstico de interfaces e características do sistema, etc. Pela sua simplicidade e conjunto de funcionalidades, esta aplicação revelou-se

ao longo deste trabalho como uma ferramenta quase de uso diário. Na Figura 3.6 é apresentada a interface do GetIf.

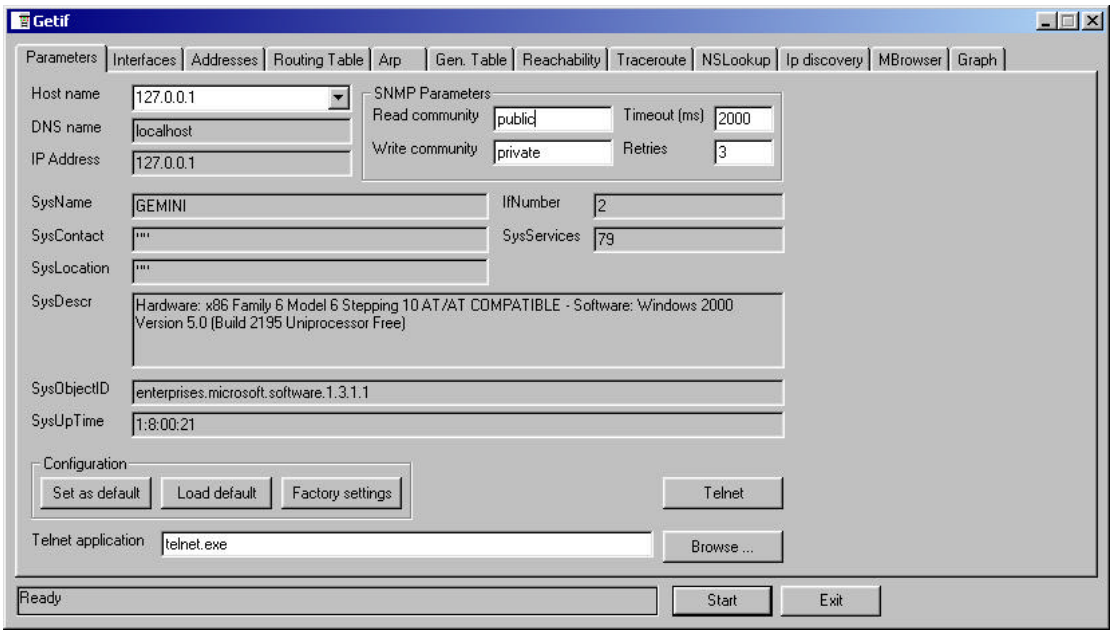


Figura 3.6 – Interface do GetIf.

A informação disponível através de alguns agentes SNMP, nem sempre é a desejada ou a mais útil. Um exemplo são os agentes SNMP implementados pelos sistemas operativos Windows, fornecem pouca mais informação, que a disponível nas MIBs normalizadas (MIB-II) [KSS00], sendo algumas variáveis, de importância vital para os gestores, por exemplo: informação relativa ao espaço em disco, à memória ocupada, ao estado dos serviços, etc. Conhecendo estes problemas a William Technology Consulting Services (WTCS), desenvolveu o SNMP4tPC [WTCS00], que não é mais que um módulo que disponibiliza as variáveis e contadores do *Performance Monitor* do Windows, através do agente SNMP. Esta informação é de extrema importância porque permite a monitorização remota de todas as variáveis que podem afectar o desempenho e a estabilidade do sistema, por exemplo, pode ser analisada a ocupação da memória ou do espaço em disco, ao longo do tempo, prevendo, atempadamente, a necessidade de mais recursos para o sistema.

3.6 Conclusão

O trabalho de análise realizado revelou-se um tanto complicado, principalmente no que respeita à disponibilização de algum do software comercial para efectuar os testes necessários. Assim a profundidade de estudo dessas aplicações não foi a desejada, tendo-se baseado quer na apresentação das aplicações, quer em artigos comparativos e opiniões de utilizadores do software.

As plataformas e aplicações de gestão, descritas anteriormente, representam apenas uma amostra do que existe neste mercado. As várias descrições efectuadas não colocam nenhuma das aplicações em vantagem competitiva, relativamente às outras uma vez que, todas elas implementam as normas de gestão actuais e um conjunto de funcionalidades semelhante, podendo eventualmente ser distinguidas pelo factor económico [TCO00a]. Por estas razões, a opção por qualquer das plataformas deve ter em conta os requisitos específicos da infra-estrutura, devendo rebuscar-se as funcionalidades que melhor respondem às necessidades, tendo sempre em conta que uma experimentação inicial das aplicações poderá ser um factor decisivo para a escolha.

Na Tabela 3.3 estão reunidas as principais características de cada plataforma, tentando facilitar a análise comparativa das funcionalidades de cada uma.

Tabela 3.3 – Tabela comparativa das plataformas de gestão de redes e sistemas.

Plataforma	Requisitos Hardware / S. O	Gestão de Redes						Gestão de Sistemas								Interface WEB	Integração com outras aplicações	Preço mínimo (€)[NWF01a]
		Descoberta automática	Gestão de Equipamentos	Monitorização remota / RMON	Processamento de Eventos	Envio de Alertas	Relatórios	DMI	CIM	DEN	Distribuição de Software	Gestão de políticas	Inventário	Controlo Remoto	Controlo de licenças			
HP OpenView NNM	HP / SUN / Intel--HP-UX / Solaris / Windows NT / 2000	✍	✍	✍	✍	✍	✍									✍	✍	5.250
Cabletron Spectrum	SUN / Intel--Solaris / Windows NT / 2000	✍	✍	✍	✍	✍	✍									✍	✍	26.300
Tivoli NetView Server	SUN / Digital / IBM / Intel--Solaris / DG-UNIX / Windows NT / 2000	✍			✍	✍	✍									✍	✍	5.300
Solstice Domain Manager	SUN / Intel--Solaris Sparc / Solaris Intel	✍			✍	✍	✍									✍		–
Unicenter TNG	Intel--Windows NT / 2000	✍			✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	300/cliente
Systems Management Server	Intel--Windows NT / 2000			✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍		50/cliente [1]
Intel LANDesk Management Suite	Intel--Windows NT / 2000				✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍		52/cliente
Spectrum Enterprise Manager com Metrix WinWatch	Intel--Windows NT / 2000 / Solaris				✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	✍	100/cliente

[1] O valor referido é reduzido para cerca de 0€ quando o produto for adquirido ao abrigo dos contratos para Instituições de Ensino

4 Caso de Estudo

4.1 Introdução

Um estudo das tecnologias e plataformas de gestão de redes e sistemas deverá ser mais do que meramente teórico, devendo ser complementado com uma análise prática das suas potencialidades. A análise da implementação requer um ambiente de estudo, que deve ser diversificado em termos de sistemas, tecnologias, aplicações, necessidades e situações, ou seja algo que exige uma grande quantidade e variedade de recursos num laboratório.

A infra-estrutura informática da Universidade de Aveiro (UA), pela sua riqueza a todos os níveis, apresenta-se como um grande laboratório, com exigências muito específicas e, por outro lado, apresenta uma série de limitações ao modo como se pode implementar uma plataforma de gestão, o que torna a infra-estrutura num ambiente de experimentação excelente.

Assim, neste capítulo será abordada a organização da UA e da sua infra-estrutura de informática e a aplicação da plataforma de gestão à mesma.

4.2 Universidade de Aveiro

A Universidade de Aveiro deu os primeiros passos na década de 70, com o curso de Engenharia Electrónica e Telecomunicações, ainda a ser leccionado em instalações cedidas pelo Centro de Estudos e Telecomunicações (CET) [UA99]. Por esta altura também a Internet iniciou a sua história, tendo surgido na UA no final da década de 80 e desde aí tem sido alvo de uma evolução contínua. A primeira rede da UA, digna desse nome, interligou o Centro de Cálculo, actual Centro de Informática e Comunicações (CIC), e o Departamento de Electrónica e Telecomunicações (DET). Seguidamente foi sendo alargada aos novos edifícios que entretanto iam surgindo e, actualmente, cobre todo o *campus* da UA. A evolução aconteceu a vários níveis, tanto na dimensão da rede, como nas tecnologias implementadas, meios de transmissão e nos equipamentos de comutação e encaminhamento.

Geograficamente a Universidade de Aveiro encontra-se numa zona mais ou menos concentrada com um diâmetro de mais de 1 km, possuindo alguns pólos e dependências instalados na região circundante, caso do centro de Aveiro e Águeda [UA00].

Na sua maioria, as Unidades da UA estão dispersas por edifícios que se encontram aglomerados no *campus* de Santiago e que possuem infra-estruturas de comunicações próprias interligadas por uma rede de espinha dorsal. Esta configuração permite à UA ajustar a rede de comunicações às suas necessidades, mantendo-a em funcionamento sem depender de serviços de terceiros, excluindo-se a esta situação o pólo de Águeda ligado à Universidade, através de um circuito de 1.4 Mbps alugado.

A infra-estrutura informática da UA tem sofrido constantes evoluções de modo a acompanhar o desenvolvimento das novas tecnologias, sendo o curso dessas evoluções pautado pela disponibilidade financeira existente em cada momento e, consequentemente, reflectindo-se numa mistura de vários meios de transmissão, equipamentos de interligação e sistemas terminais.

4.3 A Infra-estrutura de Informática da Universidade de Aveiro

A infra-estrutura informática da Universidade de Aveiro apresenta uma dimensão considerável, sendo palco de várias tecnologias e soluções que, por várias razões, coexistem, fazendo da UA um caso porventura único, no que respeita à diversidade e operacionalidade.

Nesta secção serão abordadas as características principais desta infra-estrutura analisando-se cada uma das soluções implementadas.

4.3.1 Redes Locais

O crescimento vertiginoso da Internet a que se tem assistido nos últimos anos criou nos utilizadores, e de um modo geral no mercado, a necessidade de recorrer as estas novas tecnologias. Assim é impensável qualquer edifício de uma instituição académica não possuir uma rede local de dados com ligação à Internet. As razões apontadas levaram a que todas as Unidades da UA constituíssem redes de dados locais que, na maioria dos casos, assentam sobre cablagem estruturada de categoria 5, sendo que algumas infra-estruturas, relativamente mais antigas, ainda possuem cabo coaxial e cablagem estruturada de categoria 3. Nas redes locais, e em função da dimensão dos edifícios, não pode ser considerada a existência de uma rede de espinha dorsal de edifício, sendo esta, quando existe, constituída apenas por uma ligação em fibra óptica entre dois pontos de distribuição.

Na interligação dos equipamentos terminais (computadores pessoais) são utilizados vários tipos de equipamentos de comutação, quer ao nível das suas funções quer ao nível do fabricante. Nas redes em cabo coaxial fino (RG58) ainda são utilizados repetidores na interligação dos vários troços, enquanto que nas redes em cablagem estruturada de categoria 3 e 5 a conectividade entre as várias máquinas é assegurada, na sua maioria, por concentradores de 10Mbps, existindo em alguns casos, comutadores na separação dos troços e concentradores com mais tráfego. A interligação com a rede geral é, quase sempre, assegurada por um encaminhador, restando apenas uma meia dúzia de pontes a assegurarem esta ligação.

No que concerne aos sistemas clientes, os computadores pessoais são o meio computacional mais utilizado e, na sequência de uma evolução natural, existem várias gerações em uso na UA, quer de computadores, quer de sistemas operativos, que vão desde

a família do DOS a correr sobre 386, até o Windows 2000 a funcionar sobre Pentium III. Nos sistemas servidores existem desde ambientes Novell Netware 3.12, até Windows 2000 Server, passando por Windows NT e Linux. Estes servidores fornecem os mecanismos de autenticação para os utilizadores de cada Unidades da UA, e podem ter associados serviços como o correio electrónico, partilha de ficheiros e impressoras (Figura 4.1).

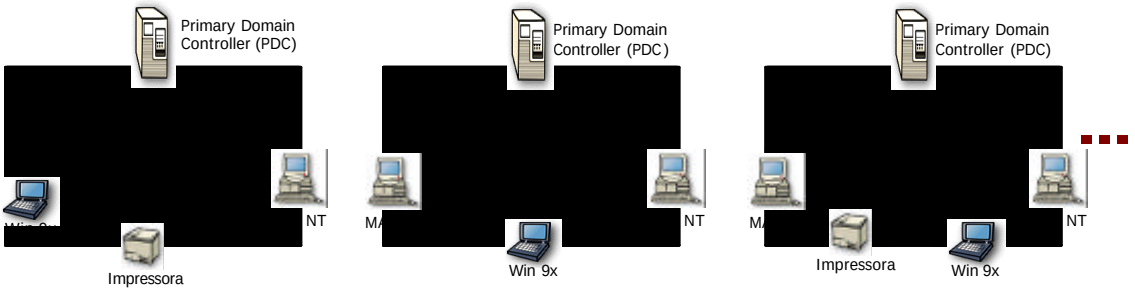


Figura 4.1 – Vários domínios NT independentes.

A heterogeneidade referida aumenta o desafio na implementação de uma plataforma de gestão que abranja a rede e os sistemas de uma forma global e integrada, sem envolver custos demasiado elevados.

4.3.2 Rede Geral

A configuração geográfica da rede da UA permite a existência de uma rede de espinha dorsal que interliga as redes locais dos diversos edifícios. Esta infra-estrutura surgiu aquando das primeiras redes locais e foi evoluindo no sentido de acompanhar os desenvolvimentos tecnológicos, sem nunca preterir as tecnologias mais antigas e em uso na Universidade, mas integrando-as o mais possível.

As razões que levaram ao surgimento de cada um dos meios físicos de suporte tiveram origens diferentes. Em primeiro lugar surgiu o cabo coaxial, como suporte à rede Ethernet que era interligado com as redes locais dos edifícios, na maioria dos casos, através de pontes, sendo o meio de transmissão com menor custo na época. Seguidamente, surgiu a fibra óptica para suportar o anel de FDDI e a rede de CATV, acompanhada pela substituição das pontes por encaminhadores, que se deveu ao baixar dos custos dos equipamentos e às características inerentes a este meio de transmissão. Mais tarde, a fibra foi sendo reaproveitada de forma a suportar a rede ATM e, por último, os novos troços Ethernet estão também instalados sobre fibra óptica, que apresenta imunidade a ruídos, maior fiabilidade e tem um custo bastante acessível.

4.3.2.1 Rede Geral – Ethernet

A rede Ethernet é neste momento a rede com maior cobertura dentro do *Campus* da UA, sendo sua maior parte, suportada por um cabo coaxial (10Base5) que se encontra em fase de migração para fibra óptica. Esta rede interliga todos os Edifícios da UA (Figura 4.2) e

em alguns casos é mesmo a única tecnologia disponível, o que torna a sua operacionalidade imprescindível. Esta operacionalidade tem sido posta em causa várias vezes, devido a descargas eléctricas sofridas pelo cabo coaxial em alturas de trovoadas, que provocam a avaria da maioria dos equipamentos ligados directamente ao cabo coaxial, o que torna urgente a migração para fibra óptica.

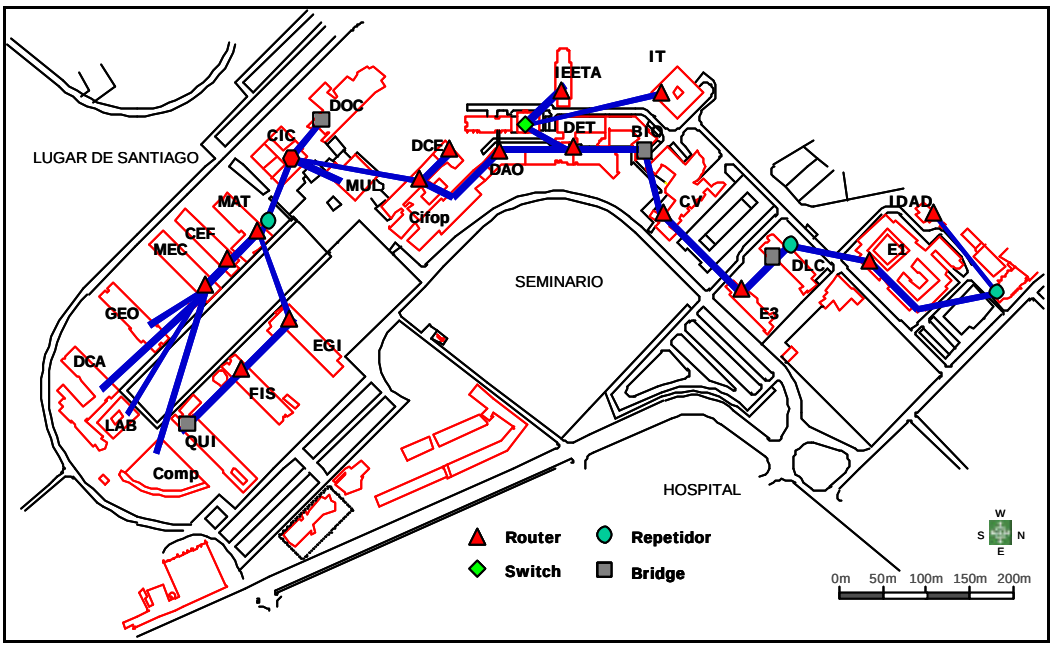


Figura 4.2 – Configuração física da infra-estrutura Ethernet.

A utilização em larga escala da rede Ethernet deve-se, essencialmente, à simplicidade de implementação aliada ao baixo custo que os equipamentos de suporte possuem quando comparados com as restantes tecnologias existentes.

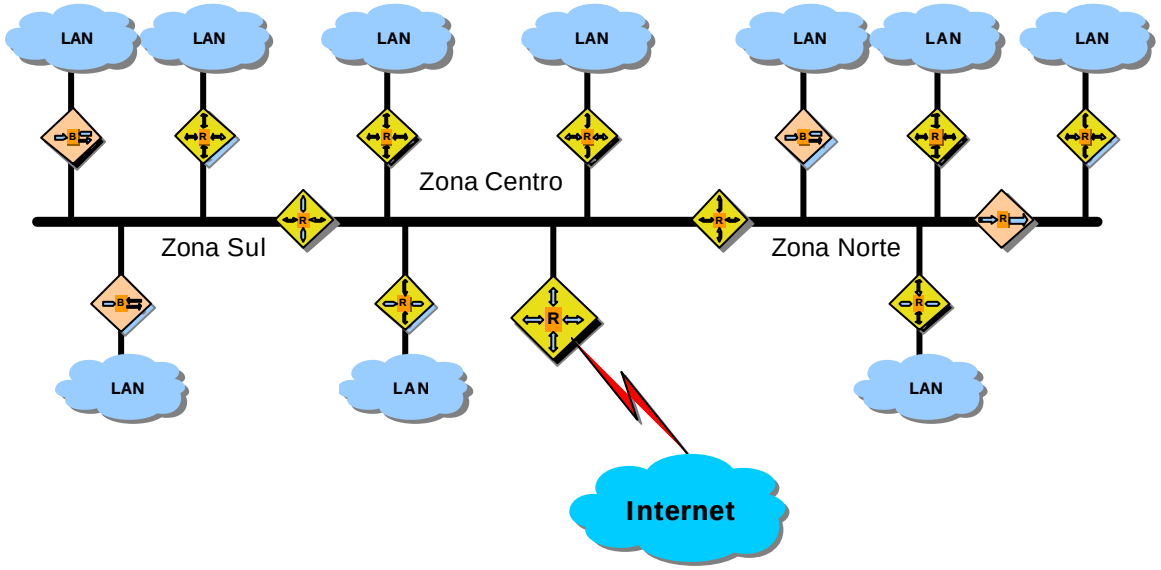


Figura 4.3 – Configuração lógica de rede geral Ethernet.

Logicamente, a infra-estrutura geral Ethernet possui uma configuração como a representada na Figura 4.3, estando a espinha dorsal segmentada em três troços, interligados por encaminhadores.

4.3.2.2 Rede Geral – FDDI

A infra-estrutura em fibra óptica (Figura 4.4) que suporta o anel FDDI foi instalada conjuntamente com o projecto FIRST, em 1994 [JAB96]. O anel constituído nessa data, interligava o CIC, o Instituto de Telecomunicações (IT) e os Departamentos de Física (FIS), Electrónica (DET) e Ciências da Educação (DCE), havendo pontos de acesso em vários outros edifícios, mas sem interligação à rede (Figura 4.5) e foi alargado recentemente ao Edifício I (E1). De notar ainda que, apesar da redundância prevista pelo FDDI, alguns procedimentos de implementação, nomeadamente o traçado das fibras e as interfaces *Single Attach* cuja alteração posterior não se justificou por ser uma solução economicamente desenquadrada do mercado, limitaram estas características.

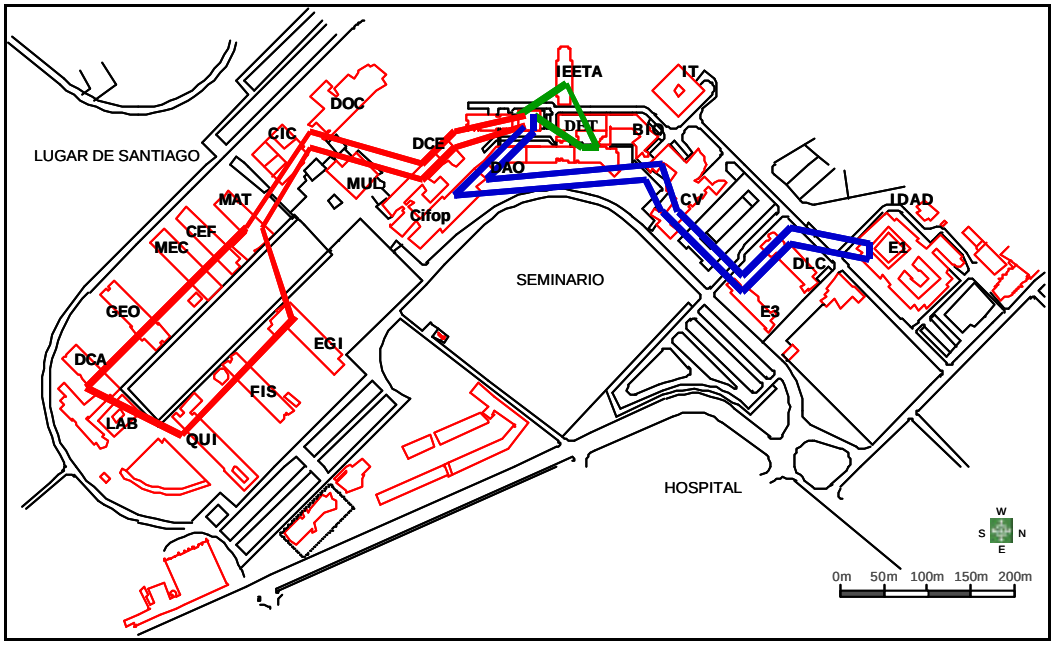


Figura 4.4 – Estrutura física do anel.

Desde a sua instalação, o FDDI servia exclusivamente a comunicação de dados entre os vários edifícios que tinham ligação à tecnologia, contribuindo para um subaproveitamento dos recursos de largura de banda e fiabilidade disponibilizados por esta infra-estrutura. Uma análise desta situação e um estudo de implementação levaram a que numa das últimas reestruturações da infra-estrutura de espinha dorsal, se efectuassem os trabalhos necessários para que o FDDI se assumisse como uma infra-estrutura de espinha dorsal transportando o tráfego dos vários troços Ethernet constituídos e já referidos anteriormente.

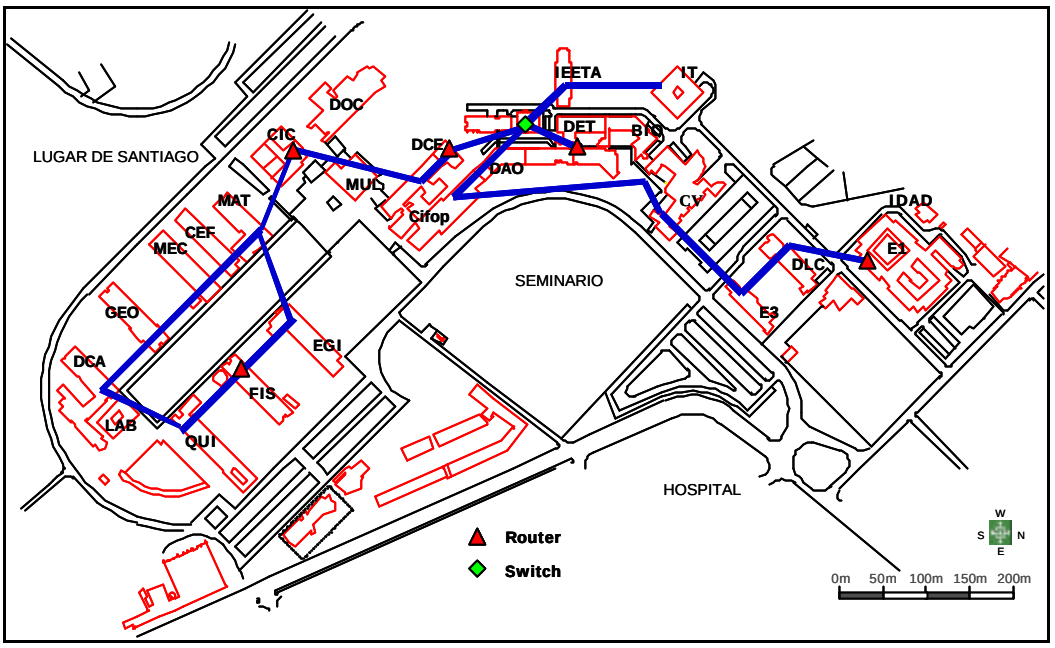


Figura 4.5 – Configuração física da infra-estrutura FDDI.

Ao contrário da Ethernet, que é utilizada na rede local dos vários edifícios, o FDDI é utilizado apenas como suporte à rede de espinha dorsal da UA, devendo-se este facto, essencialmente, ao elevado custo associado aos equipamentos terminais e de interligação da tecnologia FDDI, que não justifica a utilização generalizada desta tecnologia.

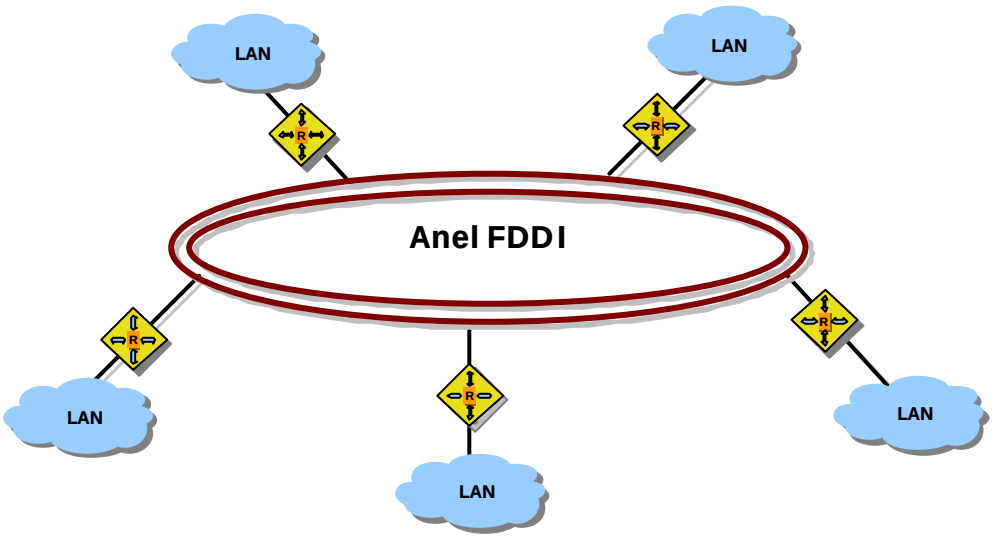


Figura 4.6 – Configuração lógica do anel FDDI.

A interligação da rede FDDI com as redes locais é efectuada através de encaminhadores com suporte FDDI e Ethernet (Figura 4.6), partilhando, o anel, uma rede lógica IP comum que assegura a comunicação entre os equipamentos.

4.3.2.3 Rede Geral – ATM

A implementação do ATM teve a sua origem na Universidade de Aveiro por volta de 1998, com uma rede experimental constituída pelo Departamento de Electrónica em colaboração com o CIC. Depois de alguns meses de experimentação, a rede experimental passou para uma plataforma de produção que serviu inicialmente o IEETA, o IT e o CIC e recentemente foi alargada ao Edifício III, onde se encontram os serviços centrais da Universidade de Aveiro.

A plataforma ATM é baseada em 2 comutadores ATM principais e estende-se desde o suporte à rede de espinha dorsal até à interligação de alguns computadores pessoais e servidores de rede. Esta rede é baseada na sua maior parte em interfaces de fibra óptica a 155Mbps no caso da espinha dorsal e UTP/RJ45 a 25Mbps e 155Mbps no caso dos servidores e máquinas pessoais (Figura 4.7).

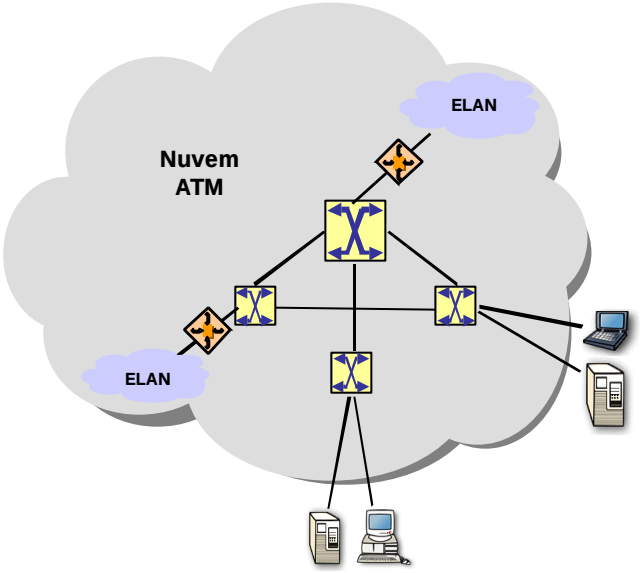


Figura 4.7 – Configuração da nuvem ATM.

As características multi-serviços do ATM não estão a ser integralmente aproveitadas, sendo esta infra-estrutura apenas utilizada para o transporte de dados. Nestas funções, o ATM transporta os dados dos edifícios que interliga e de alguns troços Ethernet, através de PVCs e SVCs, disponibilizando garantias de qualidade de serviço e uma solução escalável e adaptável às necessidades de cada momento.

4.3.2.4 Rede geral – CATV

Em 1994 foi também constituída uma rede experimental de CATV com uma rede de distribuição interna de TV na Universidade de Aveiro. A espinha dorsal desta rede é suportada por fibra óptica, sendo o sinal óptico convertido em eléctrico nos pontos de ONU e depois transportado em cabo coaxial até aos pontos de visionamento (Figura 4.8).

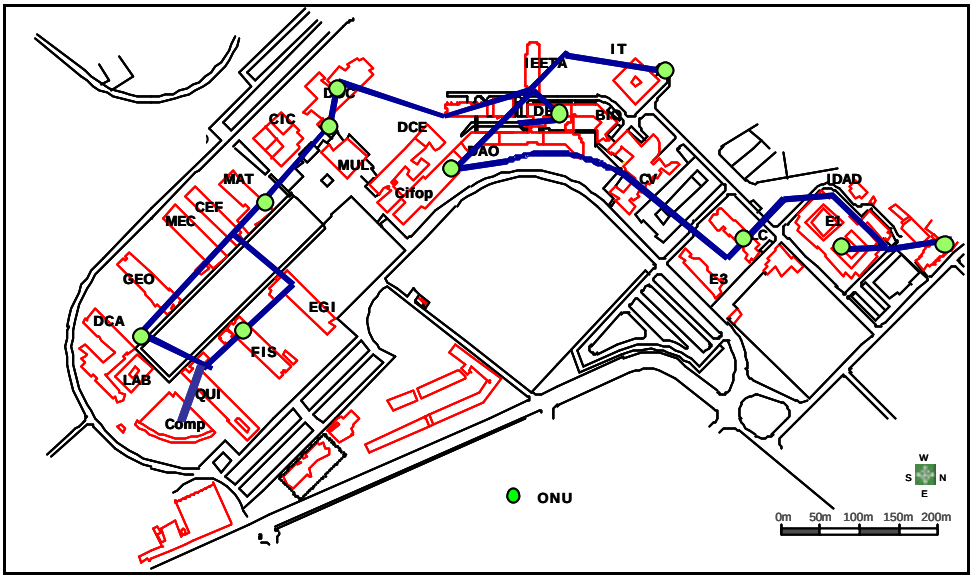


Figura 4.8 – Configuração física da rede de CATV.

4.3.2.5 Arquitectura Global

Numa perspectiva global, as várias redes físicas, descritas nos pontos anteriores, partilham a gama de endereçamento IP, organizando-se numa arquitectura esquematizada na Figura 4.9, onde se pode observar a redundância existente entre as várias tecnologias que não é dissociada de alguma complexidade da estrutura. A redundância é assegurada por várias tecnologias e caminhos físicos, geridos logicamente de um modo dinâmico pelo protocolo de encaminhamento OSPF.

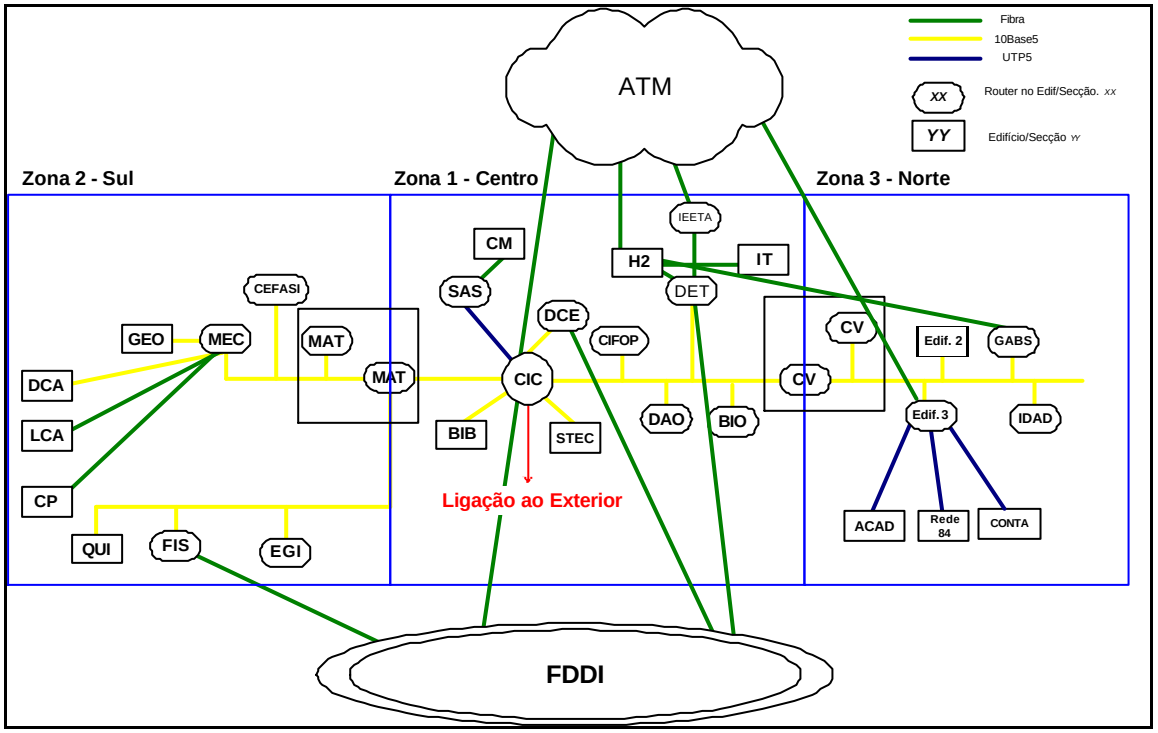


Figura 4.9 – Arquitectura global da infra-estrutura de comunicações da UA.

4.3.3 Os Sistemas

Ao nível dos sistemas, a infra-estrutura da Universidade de Aveiro pode ser vista como um conjunto de blocos independentes e autónomos na maioria das suas funções, correspondendo cada um a um edifício ou Unidade. Cada edifício possui uma intranet, fornecendo os serviços de autenticação de utilizadores, partilha de ficheiros e impressoras, correio electrónico, Web e outros, baseados quase sempre em servidores Windows NT, que permitem o funcionamento autónomo da infra-estrutura informática do Edifício/Unidade. Esta aproximação, que foi fruto da evolução da informática em geral, e em particular na UA, tem sofrido algumas mudanças passando, por exemplo, pela migração de alguns serviços para servidores centrais. Estas mudanças têm sido condicionadas pela infra-estrutura de espinha dorsal, que deverá ser beneficiada de forma a sustentar as alterações de centralização e distribuição, que melhor se adeqúem à realidade actual da UA e da informática.

Tabela 4.1 – Redes lógicas IP em uso na UA.

Redes		
Publicas	193.136.80.0	193.137.80.0
	193.136.81.0	193.137.81.0
	193.136.82.0	193.137.82.0
	193.136.83.0	193.137.83.0
	193.136.84.0	193.137.84.0
	193.136.85.0	193.137.85.0
	193.136.86.0	193.137.86.0
	193.136.87.0	193.137.87.0
	193.136.168.0	193.137.168.0
	193.136.169.0	193.137.169.0
	193.136.170.0	193.137.170.0
	193.136.171.0	193.137.171.0
	193.136.172.0	193.137.172.0
	193.136.173.0	193.137.173.0
	193.136.174.0	193.137.174.0
	193.136.175.0	193.137.175.0
Privadas	192.168.x.0	

Tentando apresentar uma perspectiva quantitativa geral, a infra-estrutura da UA é constituída por cerca de 2500 computadores e 90 servidores com uma média de idades que ronda os 2 a 3 anos, distribuídos por cerca de 40 Unidades albergadas por mais de 30 edifícios, todos eles dotados de uma infra-estrutura local de comunicações baseada em cablagem estruturada e categoria 3 e 5. Ao nível das comunicações, a UA possui 32 redes de classe C (Tabela 4.1) distribuídas pelas Unidades em simultâneo com redes privadas

para comunicação interna e serviços de Internet (http e ftp). Também são suportadas redes IPX e Appletalk em cada edifício com estes requisitos. As redes locais encontram-se interligadas pelas três infra-estruturas de espinha dorsal referidas (Ethernet, FDDI e ATM), sendo as comunicações com o exterior da UA asseguradas por um canal de 4Mbps.

Sobre esta infra-estrutura são suportados todos os serviços disponibilizados na UA, destacando-se: o correio electrónico, o WWW, o FTP, as News, o DHCP, a autenticação de utilizadores, o acesso à Internet e a partilha de ficheiros.

4.4 A Solução Aplicacional

De tudo o que foi exposto até aqui, a escolha da plataforma pode ser uma tarefa complexa, já que a oferta é muita, os preços em alguns casos idênticos e as funcionalidades semelhantes. Os únicos pontos de diferenciação são a interface de utilização que pode ser mais ou menos complexa e o modo como implementam as funcionalidades anunciadas, algo que só o contacto com a aplicação o dirá. Nesta secção serão abordadas, com algum pormenor, as aplicações sobre as quais recaiu a escolha para constituir a plataforma de gestão, tendo em conta vários factores, entre eles as funcionalidades, a facilidade de operação, o custo e a adaptabilidade à infra-estrutura da UA.

A plataforma a constituir deverá contemplar a gestão de redes e sistemas, providenciando os mecanismos mais rudimentares de construção de mapas, recolha de estatísticas de tráfego por troço/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 3COM, deverá ser acautelada a possibilidade de gerir este equipamento remotamente, retirando dele o maior partido. Finalmente a plataforma deverá apresentar um custo competitivo tendo em conta as funcionalidades oferecidas, as condições de suporte técnico e a facilidade de implementação.

Nesta perspectiva, o *OpenView NNM* satisfaz os requisitos de gestão de redes e atendendo a conhecimentos prévios, estudos de mercado existentes e aos custos associados, apresenta-se como a aplicação melhor posicionada [SEL99]. No que diz respeito à gestão dos equipamentos, a escolha foi simples, uma vez que o equipamento existente é, na sua maioria, da marca 3COM, a opção foi pelo *Transcend Enterprise Manager*. A gestão de sistemas será assegurada pelo *Microsoft SMS*, atendendo essencialmente ao custo associado, praticamente 0$/cliente, quando adquirido ao abrigo dos acordos para educação, estabelecidos com o vendedor.

A escolha mais difícil situou-se ao nível dos mecanismos de monitorização remota, RMON, que nas suas versões de hardware são extremamente dispendiosos e, nas versões de software, possuem algumas particularidades e o seu funcionamento passa a depender de

factores como o sistema operativo ou o hardware envolvido. Mesmo assim e por razões económicas a escolha recaiu sobre o *Observer Suite.*

4.4.1 OpenView Network Node Manager

Cada vez mais, os requisitos dos gestores, deixaram de ser ferramentas de gestão e passaram a ser ferramentas que, de um modo integrado, permitam gerir a diversidade de equipamentos existentes. Estes requisitos obrigaram as empresas a realizar um esforço significativo de forma a viabilizar uma resposta a esta questão. A HP não tem deixado créditos por mãos alheias e a série de produtos *OpenView* é evidência clara disso mesmo.

Na maior parte dos casos os produtos que endereçam a gestão de infra-estruturas TI, focam apenas pequenas partes desta questão. Neste âmbito, o *Network Node Manager* (NNM) pode ser visto como uma plataforma base, sobre a qual se integram vários produtos, acrescentando uma série de funcionalidades que cobrem todas as áreas da gestão.

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 NNM 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 mais rápida e eficaz, por parte do gestor.

4.4.1.1 O NNM e as Funções da Gestão

Das funções de gestão de redes, o NNM está vocacionado apenas para a gestão de falhas e problemas, a gestão de desempenho e a gestão de configurações e alterações.

Na gestão de falhas e problemas, uma das questões de mais difícil análise é a identificação rápida e efectiva da fonte de um determinado problema. Nesta área, o NNM apresenta um conjunto de características que no seu todo facilitam a tarefa, das quais se podem enumerar: a) descoberta automática dos objectos da rede e da sua topologia; b) monitorização constante dos interfaces, com envio de alertas; c) gestão de todos os objectos que implementem SNMP; d) gestão dos objectos que suportam apenas IP e/ou IPX; e) gestão de objectos que suportem DMI (bastante limitado); f) monitorização das MIBs normalizadas e privadas dos vários fabricantes; g) definição de alarmes em função de valores limite predefinidos; h) definição de acções perante a recepção de notificações; i) filtragem e correlação dos alarmes de forma a sintetizar tanto quanto possível o problema; j) possibilidade de interligação com aplicações feitas à medida das necessidades do gestor e armazenamento dos alarmes e eventos para futura análise [NNM00a].

No que diz respeito à gestão de desempenho, o NNM permite a recolha e armazenamento dos valores das variáveis das MIBs. Entre as funcionalidades que contribuem para esta gestão apresentam-se: a) colecção e armazenamento dos eventos e valores estatísticos; b)

diagnóstico e prevenção de problemas através da análise dos dados recolhidos; c) tratamento dos dados por aplicações à medida.

Na gestão de configurações e alterações, o NNM permite guardar a configuração dos equipamentos de interligação e manter um registo das mudanças de equipamentos na rede.

A complementaridade destas funções é garantida por outros produtos da família OpenView ou de terceiros, que se integram com o NNM e pelo De*veloper Kit* que permite adaptar o NNM a necessidades específicas [NNM00b], com base em programação feita à medida.

4.4.1.2 Como Funciona

O NNM, através de um sistema de eventos internos, recolhe, organiza e apresenta graficamente informação sobre todos os elementos da rede.

O NNM possui, como uma das suas maiores mais valias, uma componente gráfica que se organiza num repertório de símbolos e cores diferenciadas (Figura 4.10), possibilitando através de uma simples inspecção visual, identificar a existência de anomalias na rede. O estado dos objectos da rede é constantemente verificado pelo sistema mediante configuração efectuada, sendo as alterações reflectidas na interface gráfica [NNM00h]. Aliada à informação em tempo real, o NNM recolhe dados estatísticos e eventos ocorridos ao longo do tempo, que podem ser armazenados numa base de dados relacional, possibilitando a utilização de mecanismos de análise externos ao NNM.

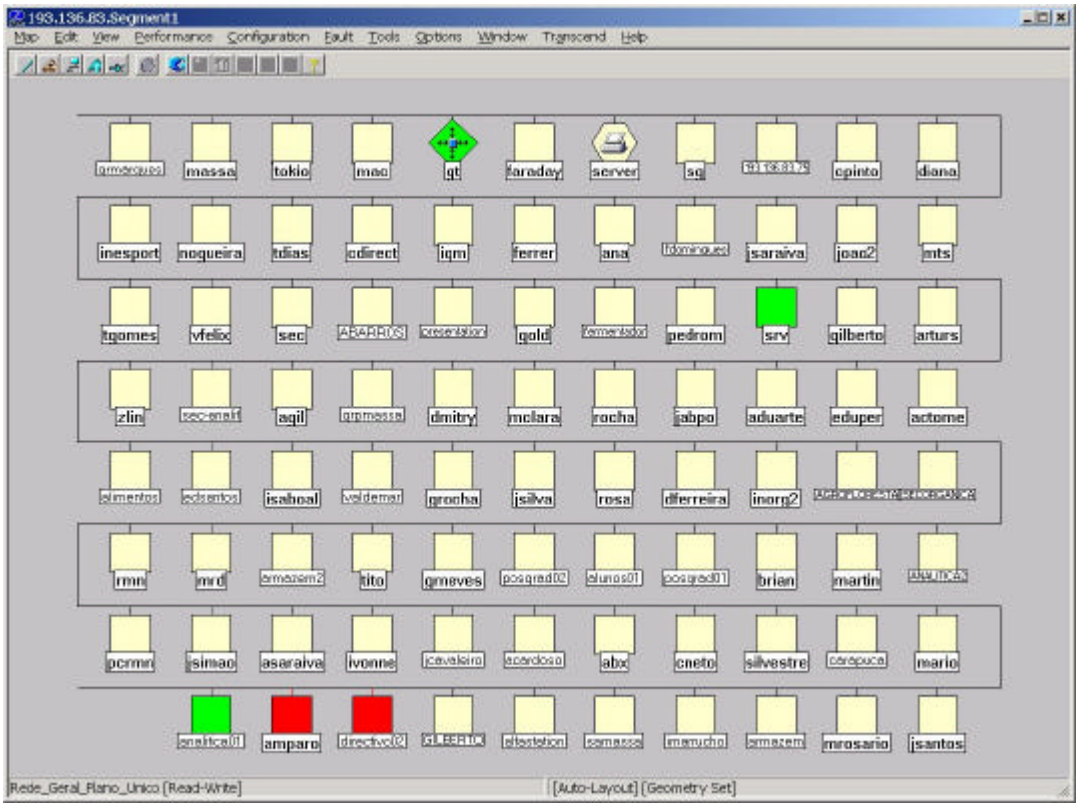


Figura 4.10 – Representação gráfica de uma rede no NNM.

Descoberta da rede

O processo de descoberta da rede, mediante a correcta configuração dos parâmetros que a regem, inicia-se identificando os objectos com conectividade e organizando-os em mapas que representam a estrutura lógica da rede.

Este processo pode demorar várias horas, dependendo da dimensão da rede e do seu correcto funcionamento e sendo condicionado pela configuração SNMP e IP dos vários nós da rede.

O processo de descoberta (Figura 4.11) tem por princípio de funcionamento a interrogação da própria LAN (1) e das tabelas ARP (2) dos equipamentos através dos agentes SNMP. Os nós são descobertos à medida que contactam com o encaminhador ou com outros nós que devolvam uma tabela ARP (2)(3), processo que se repete sempre que é escalonada uma acção de descoberta. É possível desencadear a emissão de pacotes ICMP, que inundarão toda a rede, possibilitando a descoberta dos nós que nunca se ligaram a qualquer outro equipamento SNMP.

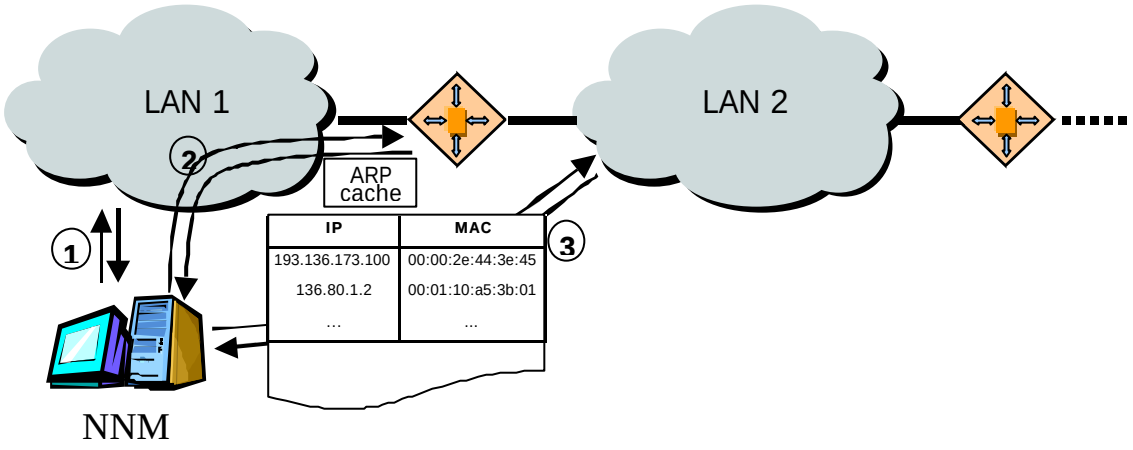


Figura 4.11 – Processo de descoberta de uma rede remota.

No caso do sistema operativo, que suporta a estação gestora, ser Windows NT também são descobertos os nós IPX da rede. Nesta situação, a descoberta baseia-se no envio de *broadcasts* para a rede de modo a identificar os vários nós IPX. Em termos de disposição gráfica é muito semelhante à anterior.

A informação recolhida até aqui, apenas permitirá identificar qual a configuração lógica da rede. Numa primeira aproximação, as redes constituídas por concentradores e comutadores comportam-se logicamente como uma rede em BUS. No entanto, se o NNM identificar alguma das MIBs, bridge (RFC 1493), repeater (RFC 2108) ou 8023MAU (RFC 1515), constrói um modelo mais fiel da interligação física dos equipamentos. A capacidade de adaptação do NNM permite a definição de outras MIBs que identifiquem equipamentos específicos e não previstos pelo NNM [NNM00h], aproximando ainda mais a representação da realidade.

Correlação de eventos

Numa rede ou troço, um problema num equipamento de interligação pode fornecer uma perspectiva errada ao gestor, se este analisar apenas os eventos ocorridos, do estado dos equipamentos do troço sem ligação. O serviço de correlação de eventos, *Event Correlation Service* (ECS), é um mecanismo que permite a detecção das causas de anomalias na rede evitando a geração de eventos redundantes, e por vezes erróneos, sobre o estado dos objectos. Por exemplo, os equipamentos que estão por trás de um encaminhador que por algum motivo está em baixo, encontram-se apenas inacessíveis e logo num estado desconhecido, pelo que até à ligação ser reposta não será gerado nenhum evento sobre o estado desses equipamentos (Figura 4.12).

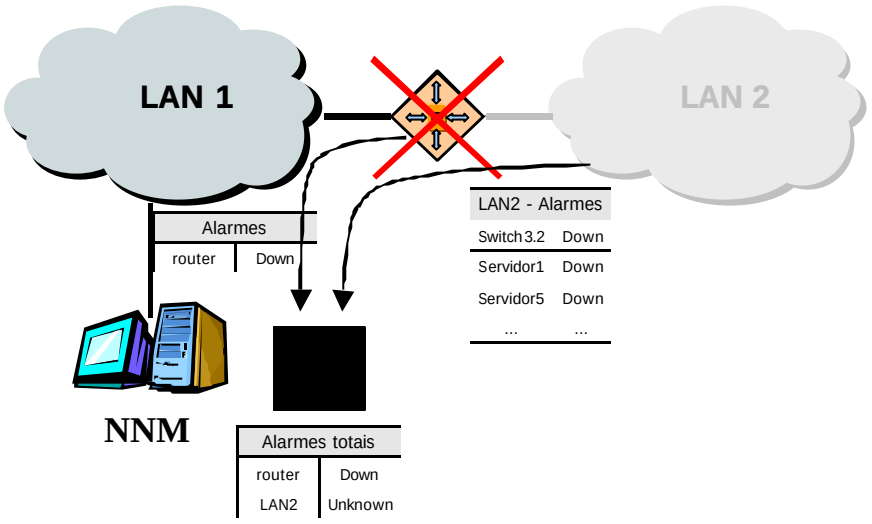


Figura 4.12 – Processo de correlação de Eventos.

O ECS já se encontra pré-configurado no NNM mas pode ser alterado através de uma interface Web, de modo a adaptar-se às alterações efectuadas nos equipamentos de rede. O ECS é um mecanismo implementado também por outras aplicações da HP, integrando-se como um todo numa plataforma constituída por soluções HP [HPOV00a].

As bases de dados

Toda a informação recolhida pelo NNM assim como a informação gerada por ele, nomeadamente mapas e eventos próprios, é armazenada numa base de dados interna, que pode ser subdividida em cinco componentes distintas (Figura 4.13): a) objectos, b) topologia, c) mapas, d) eventos e) estatística. No entanto, por ter um formato próprio, esta base de dados não é acessível por nenhuma ferramenta de manipulação de bases de dados externa, sendo manipulada apenas pelo NNM [NNM00e].

Para colmatar esta dificuldade o NNM possui ferramentas que possibilitam a exportação da informação para bases de dados relacionais, dos quais são exemplos o SQL e o Oracle. Estas bases de dados relacionais permitem o armazenamento do historial da rede para

posterior análise, melhorando o desempenho da estação gestora que fica liberta para as funções de gestão, sem ter de processar a base de dados.

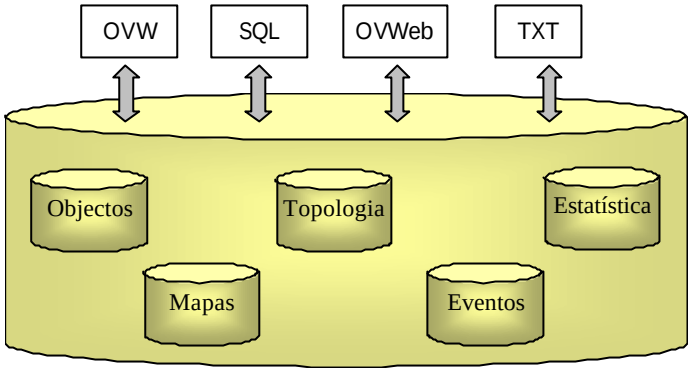


Figura 4.13 – Base de dados internas ao NNM

4.4.1.3 Verificação do Estado dos Objectos

Após uma fase inicial onde são descobertos os objectos da rede, o NNM verifica periodicamente o estado dos objectos. Esta verificação provoca tráfego na rede e os tempos entre duas verificações sucessivas deve ser estipulado de acordo com a importância do objecto e com os limites do tráfego a ser gerado pela estação gestora, de modo a não saturar a rede com informação de gestão.

Os parâmetros podem ser configurados para conjuntos de objectos ou objectos individuais permitindo um controlo efectivo do tráfego gerado pela aplicação de gestão (Figura 4.14).

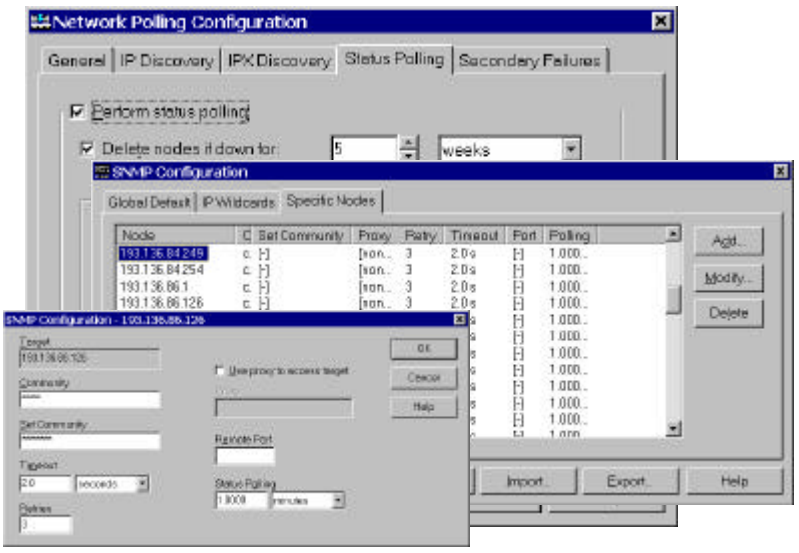


Figura 4.14 – Janela de configuração da verificação do estado dos equipamentos.

O estado dos objectos é representado por um esquema de cores que, através de uma simples inspecção visual, permite uma perspectiva global do estado da rede. Este esquema

de cores está dividido em vários níveis representando cada um o estado de um objecto a dado momento (Figura 4.15).

Figura 4.15 – Estados dos objectos.

4.4.1.4 Objectos e Sua Organização

Objectos e símbolos

No NNM, um objecto representa um recurso de rede passível de ser gerido e possui um conjunto de atributos que modelam a entidade gerida. Estes objectos são representados nos sub-mapas a que dizem respeito através de símbolos, assim os símbolos são representações gráficas dos objectos, que podem existir em vários sub-mapas (Figura 4.16). Para além da representação dos objectos, aos símbolos está associada a navegação nos mapas, a execução de acções e a indicação do estado do objecto.

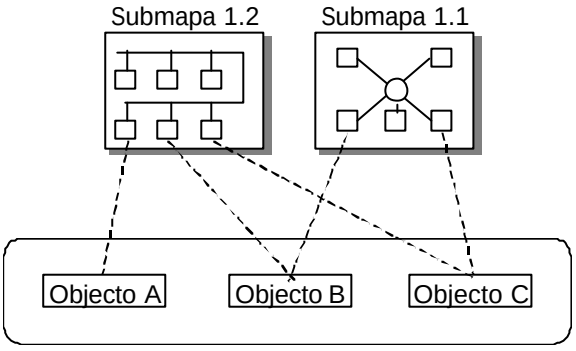


Figura 4.16 – O mesmo objecto em vários mapas.

Existem dois tipos de símbolos, os ícones e as ligações, representando respectivamente os equipamentos da rede e as ligações estabelecidas entre eles.

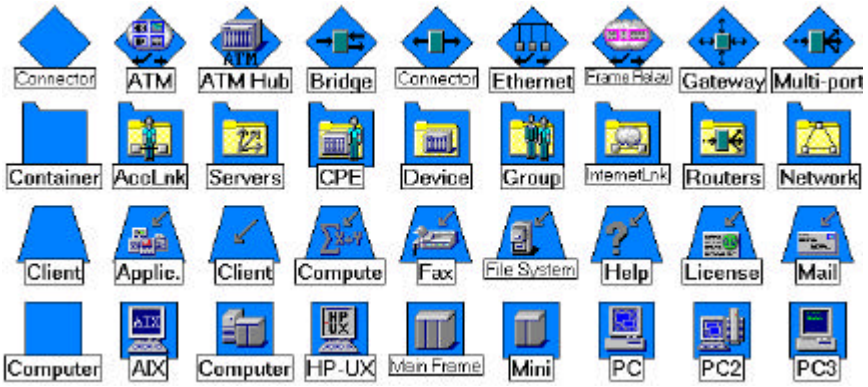


Figura 4.17 – Símbolos predefinidos no NNM.

O NNM traz um conjunto de símbolos predefinidos (Figura 4.17) que pode ser enriquecido acrescentando novas definições ao ficheiro de configuração, à medida das necessidades da instituição.

Mapas

O NNM organiza a informação relativa à topologia da rede em mapas e sub-mapas, sendo a relação entre estas duas componentes comparável à de um Atlas e as suas páginas. Assim, os mapas são representações gráficas de conjuntos de objectos organizados mediante determinados critérios, referindo-se a diferentes domínios de gestão, objectos e localizações.

Para uma determinada sessão do ovw (interface do NNM), apenas um mapa pode estar aberto. Caso seja necessário manter mais mapas abertos, poderão iniciar-se diferentes instâncias do ovw, uma por cada mapa.

Em cada mapa os objectos apresentados são apenas símbolos que referenciam objectos constantes das bases de dados; não existe duplicação de informação, uma vez que os objectos são sempre os mesmos.

Sub-mapas

Os sub-mapas, por sua vez, representam vistas particulares de um mapa e apresentam numa mesma janela os objectos com características comuns. Os sub-mapas podem ser entendidos como os elementos constituintes de um mapa organizados hierarquicamente, não existindo limite para o número de sub-mapas abertos numa sessão. Particularizando, os sub-mapas podem reflectir a estrutura da organização, do espaço físico, a configuração lógica da rede ou qualquer outro factor que importe representar (Figura 4.18). Com este intuito é possível configurar vários parâmetros para cada sub-mapa, por exemplo, atribuir-lhe uma imagem de fundo ou um filtro, tornando mais perceptível a organização que se pretende modelar.

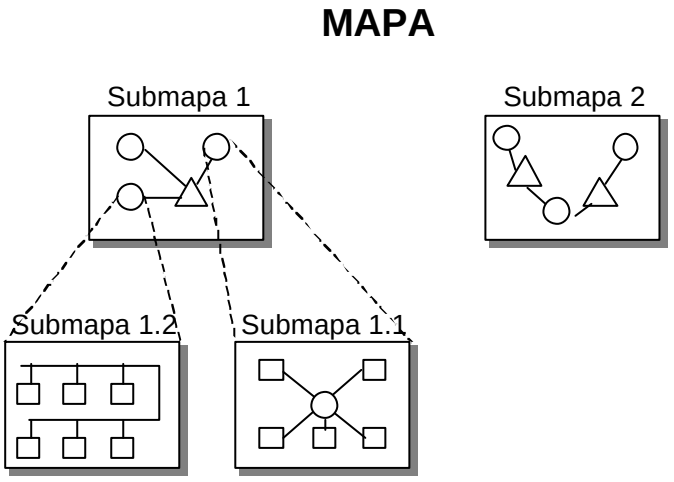


Figura 4.18 – Agrupamento dos objectos em sub-mapas.

O NNM possui algoritmos que dispõem os símbolos nos sub-mapas de acordo com o tipo dos objectos que estão envolvidos. No entanto, é possível desactivar esta função, passando o gestor a adaptar o grafismo dos sub-mapas a situações particulares [NNM00h].

Filtros

Numa organização com uma rede complexa e de grande dimensão pode ser necessário e conveniente filtrar a quantidade de informação que é mostrada ao gestor. Neste sentido, o NNM inclui a possibilidade de definir e utilizar filtros que limitem a informação visualizada (Figura 4.19).

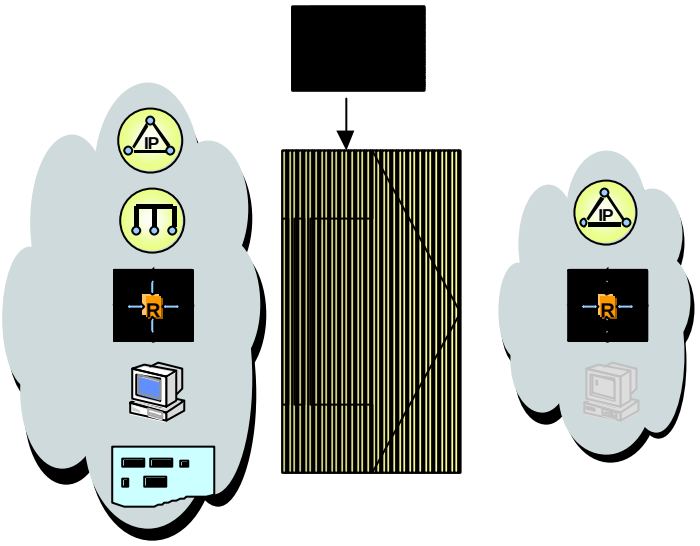


Figura 4.19 – Aplicação de filtros aos mapas.

Estes filtros são definidos num ficheiro de texto e podem adaptar a dimensão visual dos mapas à medida das necessidades de cada gestor. Os objectos depois de submetidos aos filtros podem ainda ser ocultados no mapa, realçando os objectos que se pretendem representar.

O conjunto destas duas funcionalidades, possibilita a configuração visual do mapa no seu todo e dos sub-mapas individualmente, fornecendo a cada gestor apenas a informação que necessita, sem uma sobrecarga de informação desnecessária [NNM00d].

Organização dos sub-mapas

A informação recolhida pelo NNM é organizada segundo algoritmos internos numa estrutura hierarquizada segundo os níveis: a) Topo, b) Internet, c) Rede, d) Segmento e) Nó (Figura 4.20), aos quais correspondem diferentes papéis. O nível de topo contém os mapas que sendo independentes são acessíveis a partir deste nível. O nível Internet é o mais flexível em termos de configuração, sendo aqui modeladas todas as realidades que se pretendam representar. O nível de rede contém os equipamentos de interligação e os segmentos que façam parte da rede lógica em questão. O nível do segmento contém os

objectos correspondentes aos equipamentos individuais com endereçamento atribuído. O nível do nó contém as interfaces físicas integrantes do equipamento.

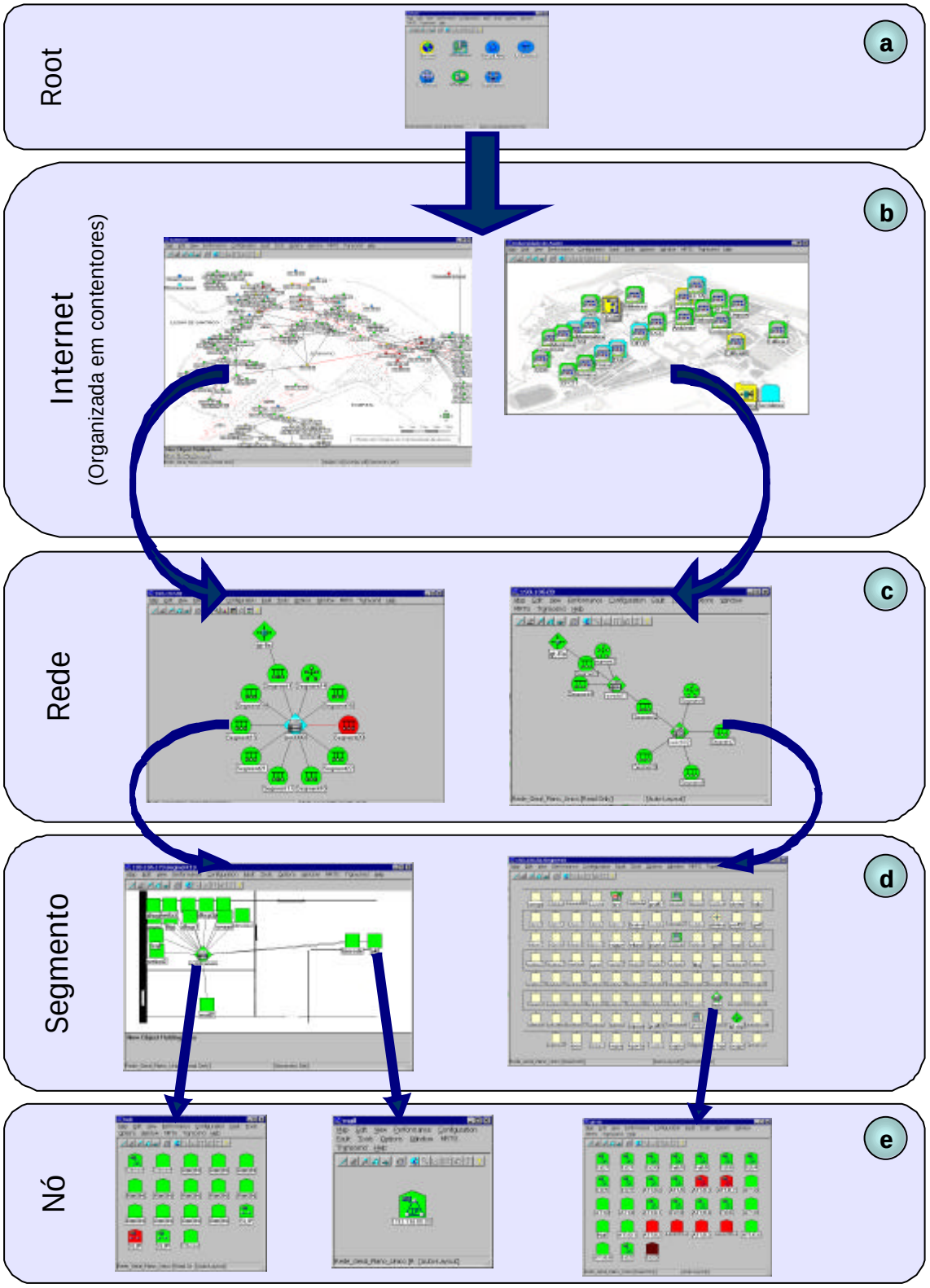


Figura 4.20 – Os vários níveis organizativos do NNM.

Como foi referido, o nível Internet possui algumas características particulares que se podem traduzir na capacidade de criar contentores com a função de aglutinarem os objectos, organizados de modo a permitir modelar uma realidade física ou orgânica da instituição. Aqui os contentores de objectos podem ser criados, eles próprios dispostos em vários níveis garantido uma grande flexibilidade na sua organização (Figura 4.21).

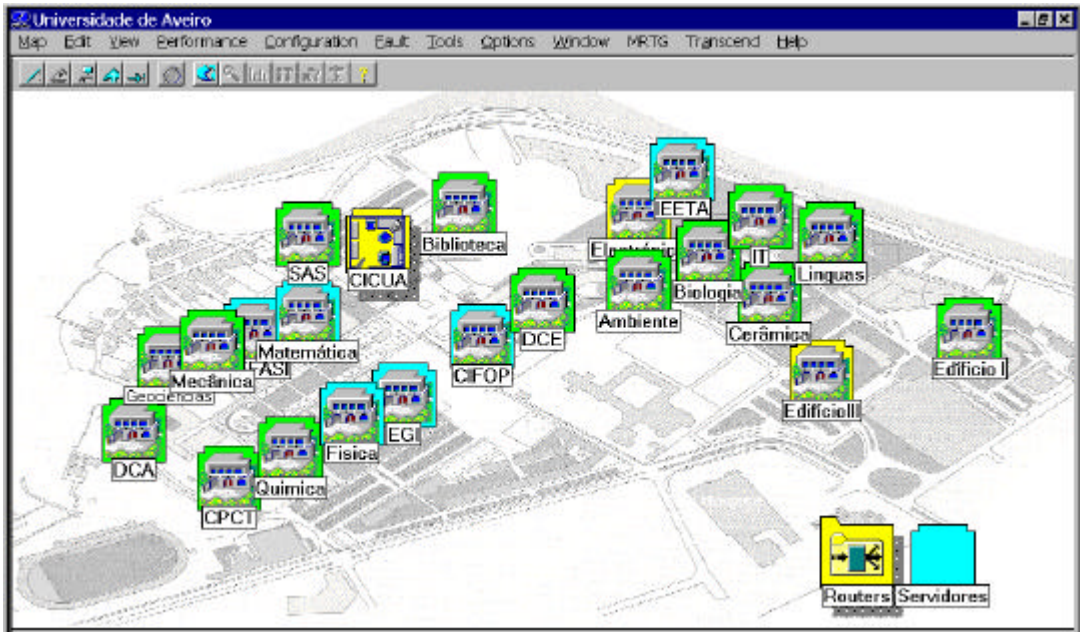


Figura 4.21 – Organização física da infra-estrutura.

4.4.1.5 Acesso à Estação Gestora

A política de acesso à estação gestora deverá ser cuidada atendendo às funcionalidades pretendidas e à protecção da informação constante da base de dados, que inadvertidamente acedida, pode colocar em causa pontos sensíveis da organização. Uma descrição pormenorizada sobre as políticas de controlo de acessos pode ser encontrada em [NNM00d].

Controlo de acesso aos Mapas

Quando as dimensões da organização justificam a distribuição das tarefas de gestão por várias pessoas é necessário ter em conta as áreas de actuação de cada uma, de modo a não haver colisões e atropelos entre as operações efectuadas.

O NNM resolve a questão anterior através da definição de menus específicos para cada utilizador ou grupo, implementando segurança ao nível do sistema de ficheiros, que no caso do Windows NT é assegurado utilizando o sistema NTFS (Figura 4.22).

As funcionalidades enumeradas darão ao gestor um conjunto de ferramentas adequadas às funções que irá desempenhar, garantindo simultaneamente o controlo de acesso à informação estritamente necessária para as tarefas a desempenhar.

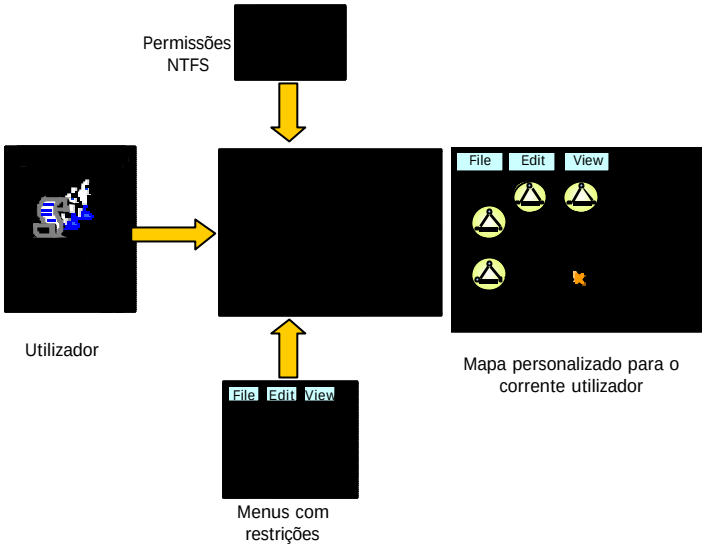


Figura 4.22 – Controlo de acesso à estação gestora.

Controlo de acesso ao NNM

O acesso à estação gestora pode ser efectuado remotamente eliminando a necessidade de se estar em frente da consola e permitindo que vários utilizadores acedam à aplicação simultaneamente, a partir de qualquer ponto da rede.

Dos vários acessos que se podem utilizar contam-se: a) o acesso através da interface WEB disponibilizada pelo NNM, b) o acesso através de uma consola remota que necessita de instalação nos clientes, c) no caso de um NT Terminal Server o acesso através de uma consola do Terminal Server que apenas requer a presença do cliente Terminal Server (Figura 4.23).

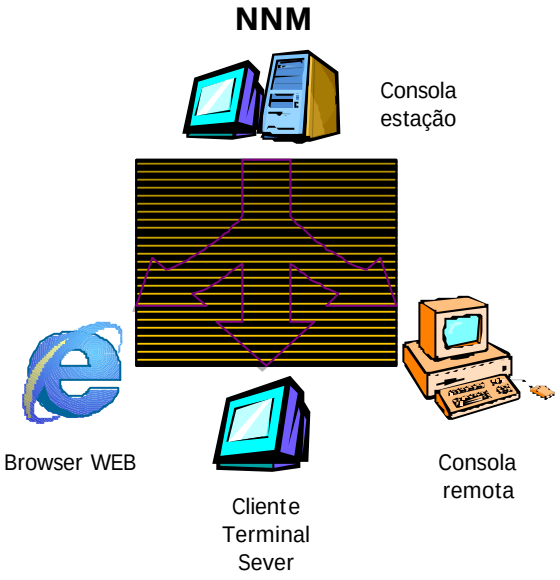


Figura 4.23 – Acesso a partir de múltiplas plataformas.

4.4.1.6 Interface WEB

No estado de desenvolvimento actual das tecnologias de informação, a existência de uma interface WEB para qualquer aplicação é requisito quase obrigatório. Aliás, sendo esta uma lacuna das versões anteriores, foi desenvolvida, no âmbito de projecto de final de licenciatura, uma interface baseada em JAVA que disponibilizava parte da informação da aplicação NNM versão 4.2 [RSJ98a]. A partir da versão 5, o NNM disponibiliza também uma interface que permite o acesso através de um browser WEB, a praticamente todas as funcionalidades disponibilizadas e acessíveis através da interface *ovw* da estação gestora (Figura 4.24).

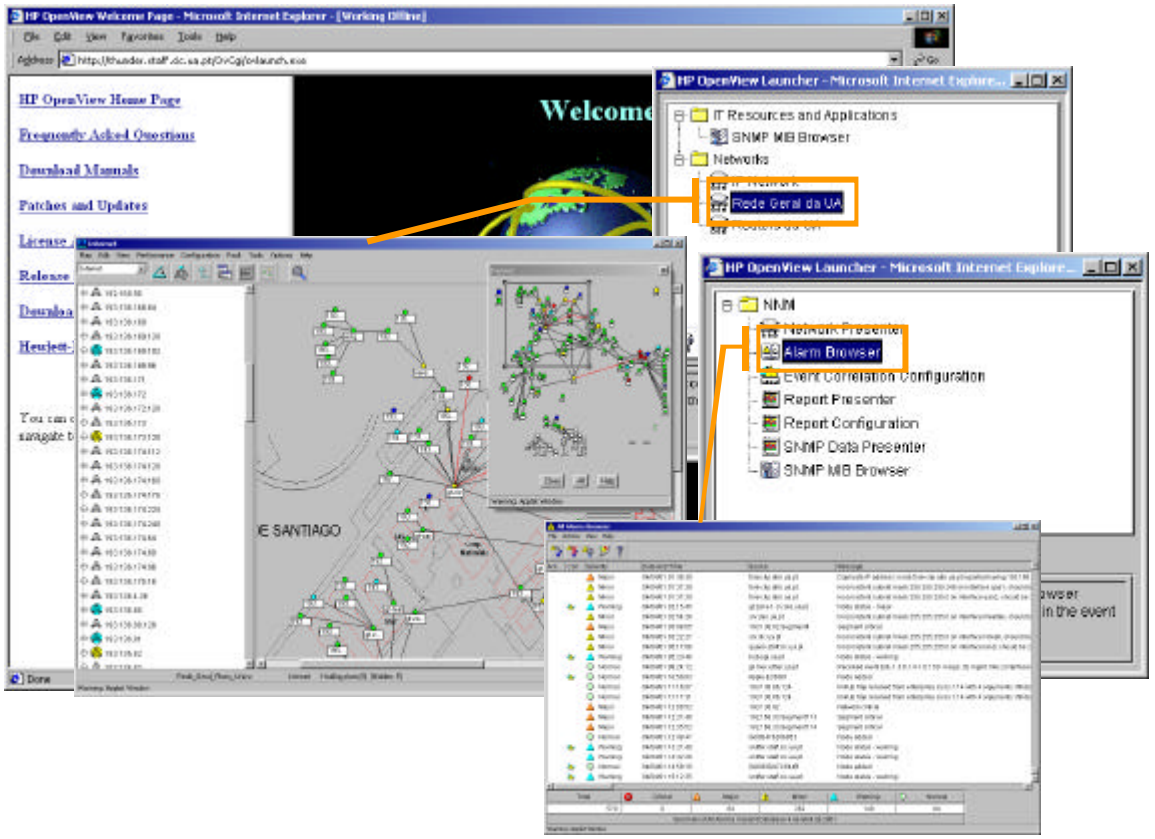


Figura 4.24 – Interface Web do NNM.

A interface do NNM é baseada em JAVA e constituída por um conjunto de *applets* que interagem com os módulos correspondentes na estação gestora. Sendo susceptível de uma série de configurações, tal como acontecia para os módulos do NNM, esta interface permite também a adequação da informação aos utilizadores que a vão consumir. Os utilizadores podem estar divididos em vários níveis correspondendo a cada um uma responsabilidade diferente na gestão da infra-estrutura.

A instalação e a configuração da interface Web são feitas automaticamente, com a instalação do NNM, podendo-se depois ajustar a configuração às necessidades concretas da implementação. As alterações à configuração são efectuadas actuando sobre os ficheiros de

registo, WLRF's, que personalizam a interface e, conjugados com os ficheiros de acesso, disponibilizam funcionalidades diferentes a cada gestor [NNM00g].

4.4.1.7 Sistema de Eventos

Todo o funcionamento do NNM assenta sobre um sistema de eventos que garantem a consistência da informação. Na Figura 4.25 são apresentados o relacionamento e interacção dos vários componentes do NNM.

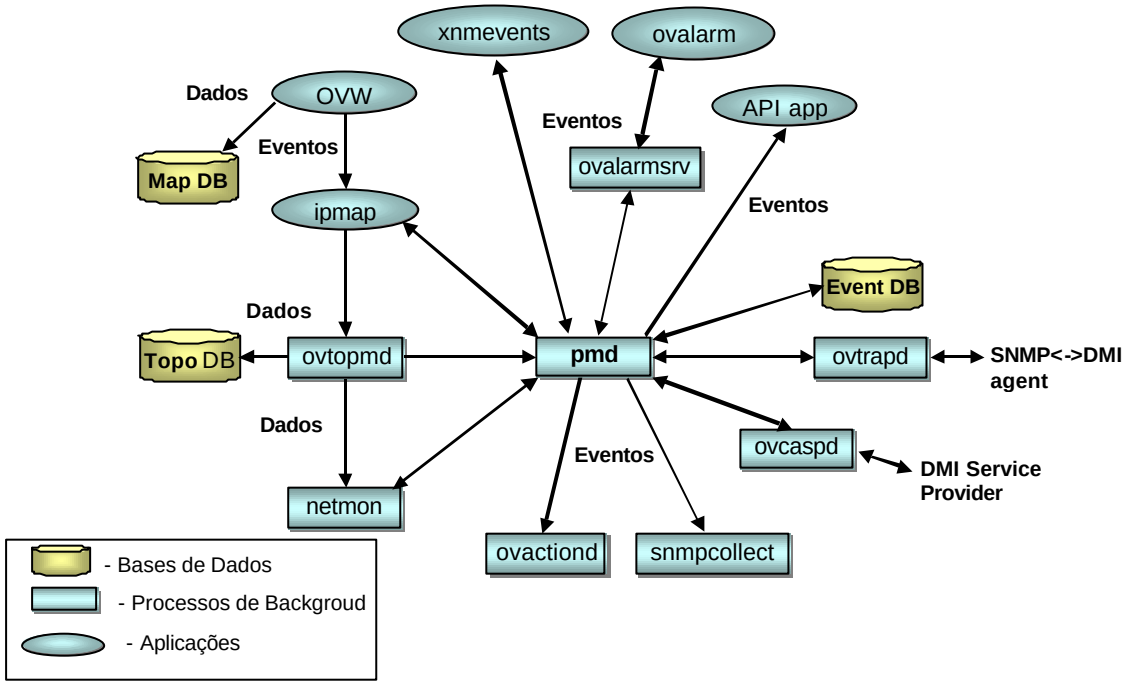


Figura 4.25 – Funcionamento do sistema de eventos.

Todos os eventos são passados ao processo *pmd* que os envia para a base de dados de auditoria e para as aplicações que os subscrevem. Quer isto dizer que nem todos os eventos são mostrados no Browser de Eventos, sendo apenas utilizados para processamento interno do NNM [NNM00h].

Base de dados de MIBs

Assentando a base da comunicação do NNM sobre o SNMP, é premente a necessidade de conhecer as MIBs normalizadas e as que são implementadas pelos fabricantes, de modo a ser perceptível a informação armazenada pelo NNM na sua base de dados de eventos.

No sentido de facilitar o manuseamento das MIBs, existem algumas ferramentas (Figura 4.26) que possibilitam o carregar e descarregar de MIBs da base de dados permitindo, através do MibBrowser, a visualização e navegação pela estrutura de informação disponibilizada pelos agentes SNMP implementados nos equipamentos.

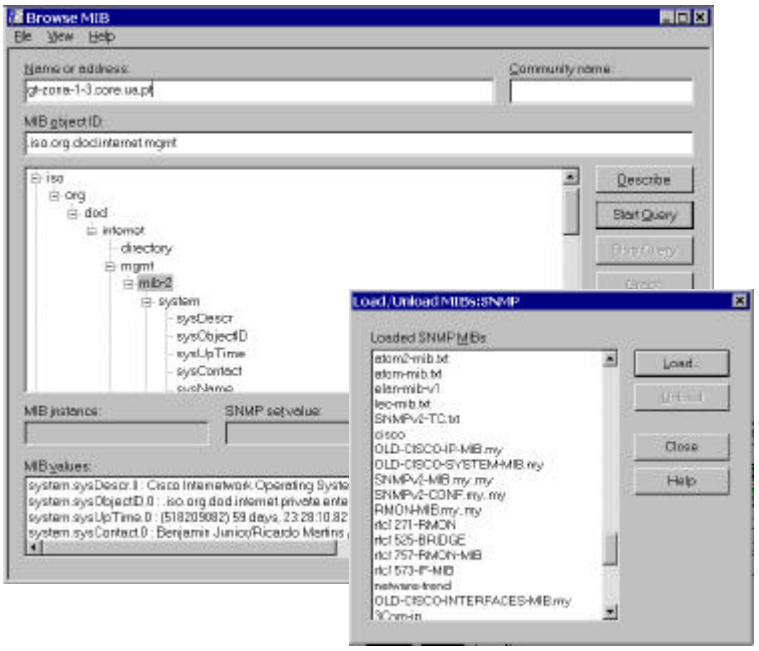


Figura 4.26 – MibBrowser e interface de carregamento de MIBs.

Configuração de eventos

Os eventos já se encontram pré-configurados aquando da instalação do NNM mas, para cada caso, podem ser ajustados às necessidades concretas do gestor. Assim, podem ser adicionados mais eventos para uma situação específica, ou ajustados os parâmetros dos eventos pré-configurados, de forma a responder às necessidades existentes.

A configuração de um evento passa pela definição do identificador do evento, do nome do evento, das acções a tomar e pela definição das fontes do evento, ou seja, a definição dos objectos para os quais deve ser tido em conta o evento (Figura 4.27).

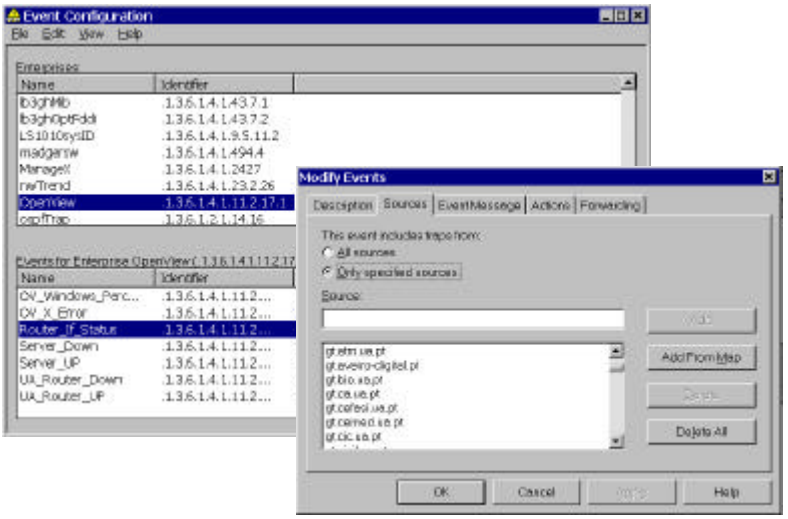


Figura 4.27 – Eventos e janela de configuração.

Depois de recebido um evento, as acções que podem ser tomadas relacionam-se com o tipo de armazenamento que irá ser feito deste evento, com a mensagem que será gravada na base de dados e com as aplicações que podem ser lançadas mediante a recepção do evento. A mais comum é uma aplicação de envio de mensagens de correio electrónico a alertar o gestor responsável pelo equipamento.

Colecção de dados estatísticos

O armazenamento do historial de determinadas variáveis das MIBs permite uma posterior análise com uma consequente definição de procedimentos e políticas que potenciem elevados níveis de desempenho da rede e dos sistemas.

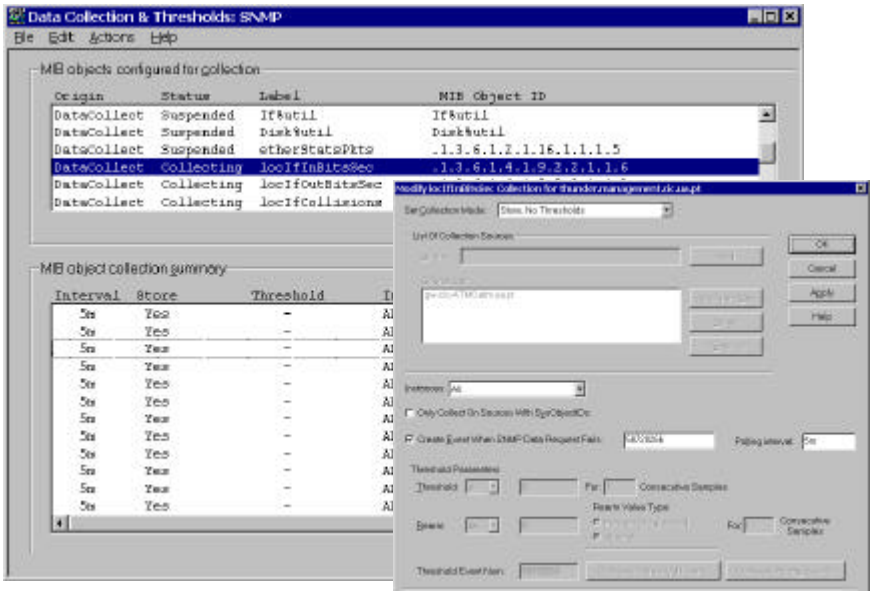


Figura 4.28 – Configuração da colecção de dados estatísticos.

Tendo em atenção este facto, o NNM disponibiliza uma interface onde podem ser configuradas quais as variáveis que se querem monitorizar, a partir de que fontes e com que intervalo de tempo entre medidas sucessivas, para além de permitirem a definição de limites, a partir dos quais podem ser desencadeadas acções de alerta ou outras (Figura 4.28). A colecção de estatísticas é um processo que provoca tráfego na rede, devendo ser cuidado na sua implementação e utilizado apenas em pontos-chave ou essenciais para a gestão de infra-estrutura.

Os Módulos do NNM

Neste ponto serão abordados os componentes aplicacionais que constituem o NNM, bem como a sua relação e interdependência, tentando ilustrar o seu funcionamento interno.

O NNM funciona através de uma série de módulos que são executados em modo de serviço e através de aplicações que funcionam em modo interactivo. A Figura 4.29 esquematiza o funcionamento dos componentes que iniciam a operação da plataforma, sendo referidos os ficheiros de configuração que são tidos em conta nesta fase e, consequentemente, regularão o funcionamento dos vários componentes [NNM00h].

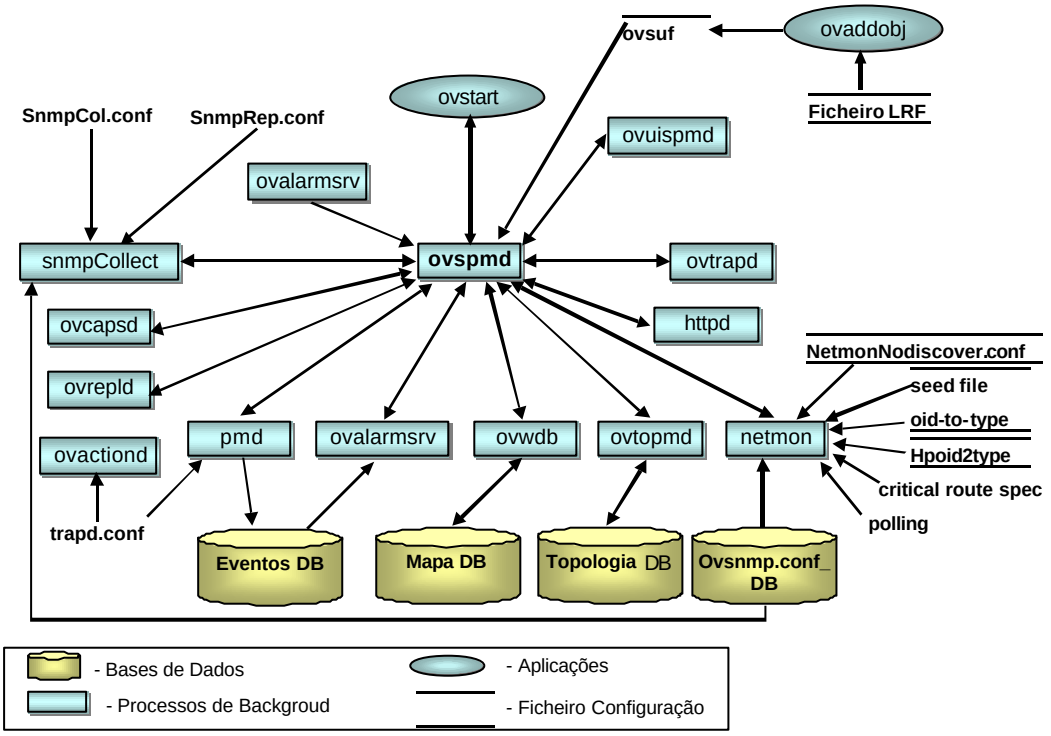


Figura 4.29 – Módulos do NNM no arranque.

Nas Tabelas 4.2, 4.3 e 4.4 são apresentados os principais serviços e aplicações, assim como uma breve descrição das suas funções, necessária à percepção da modularidade da plataforma e à análise e diagnóstico de problemas com os módulos do NNM.

Tabela 4.2 – Aplicações WEB.

Aplicação	Função
jovw	Equivalente ao ovw, inicia a sessão
ovalarm	Lança o visualizador de eventos
snmpviewer	Possibilita a visualização gráfica dos dados recolhidos na estação gestora

Tabela 4.3 – Aplicações gráficas do NNM.

Aplicação	Função
ipmap	É executada aquando do ovw e é responsável pela representação gráfica dos mapas
ovw	Aplicação que faz o interface entre os serviços do NNM e o utilizador
xnmbrowser	Permite efectuar a visualização do valor das variáveis das MIBs (MIB Browser)
xnmevents	Interface que possibilita a visualização dos eventos e alarmes recebidos
xnmgraph	Ferramenta que possibilita a visualização gráfico dos dados estatísticos recolhidos
xnmloadmib	Pode ser utilizada para fazer a análise das MIBs e carregá-las para memória
xnmcollect	Permite configurar de quais as variáveis serão recolhidos os dados estatísticos
xnmtrap	Aplicação que permite gerir e configurar o sistema de eventos

Tabela 4.4 – Serviços do NNM.

Módulo	Função
ovstart	Inicia os vários módulos do NNM
ovspmd	Lança todos os serviços e gere a interacção entre eles e as operações solicitadas pelo utilizador
httpd	Recebe os pedidos de http efectuados pelos clientes WEB
netmon	Responsável por efectuar a descoberta da rede e por manter actualizada a base de dados com o estado dos objectos
ovactiond	Recebe eventos do pmd e executa os comandos associados
avalarmsrv	Providencia a informação sobre os alarmes para o Browser WEB baseado em JAVA
ovcaspd	Fica à espera de novos nós e verifica as suas capacidades em termos de SNMP, DMI, ...
ovrepld	Responsável pela replicação de objectos num ambiente distribuído
ovrequestd	Executa a exportação da informação para a Data WhareHouse e realiza os relatórios em tempos pré definidos
ovsessionmgr	Gere as sessões WEB existentes
ovtopmd	Mantém a base de dados de topologia, que consiste num conjunto de directórios e ficheiros que contém a informação sobre a organização e o estado dos objectos de rede
ovtrapd	Recebe os Traps SNMP e envia-os para o pmd
ovuispmd	Gere a resposta aos pedidos efectuados pelos utilizadores das sessões ovw
ovwdb	Gere a base de dados de objectos
pmd	Gere a recepção e envio de eventos para a base de dados e para os vários processos
snmpCollect	Colecciona as variáveis das MIBs pré configuradas e armazena-as na base de dados correspondente

Na Figura 4.30 encontra-se ilustrada a relação entre os componentes que fazem parte da operação normal do NNM, esquematizando-se a interacção com a base de dados e com os ficheiros de configuração, cujas alterações são reflectidas automaticamente no funcionamento do NNM.

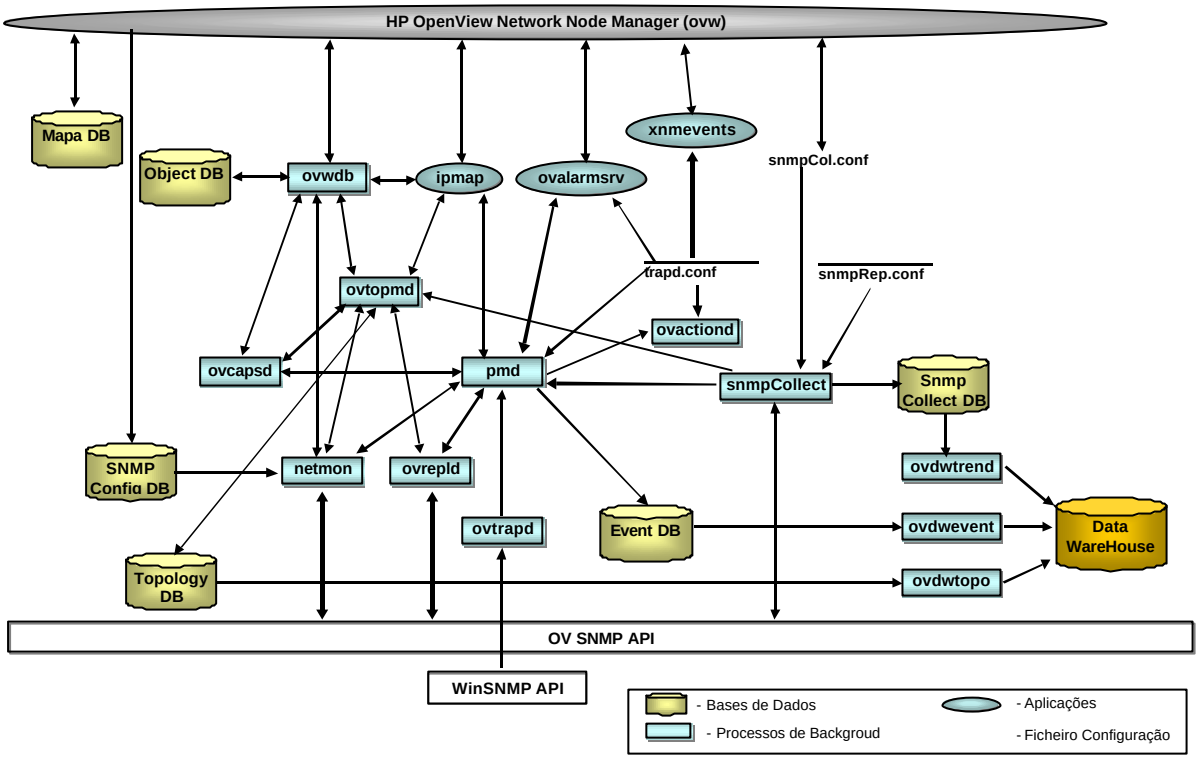


Figura 4.30 – Funcionamento do NNM.

A Figura 4.31 ilustra o funcionamento das aplicações e serviços que fazem parte do servidor Web, que disponibiliza o acesso à estação gestora através de um browser Web.

4.4.1.8 Os Ficheiros de Configuração do NNM

A configuração de todos os serviços de NNM é feita tendo por base ficheiros de texto com os parâmetros de iniciação dos vários processos. Estes são armazenados nos directórios \openview\conf\, \openview\lrf\ e \openview\www\registration\launcher\C. O primeiro processo a iniciar é o *ovspmd* que utiliza o ficheiro *ovsuf* onde estão definidos os restantes processos e os seus parâmetros, configurados através dos *Local Registration File* (LRF). Os LRF's definem os parâmetros correspondentes a cada serviço, e através do comando *ovaddobj* são adicionados ao *ovsuf* fazendo com que, da próxima vez que os serviços forem iniciados, as alterações se reflictam na operação do NNM. Para além destes RF's, existem ainda os *Application Registration Files* (ARF) e os *Web Launcher Registration Files* (WLRF), responsáveis pela configuração das aplicações e da interface Web, respectivamente [NNM00g]. A nomenclatura dos RF's é formada pelo nome do serviço seguido da extensão do correspondente RF (Ex: *netmon.lrf*, *ovtopmd.lrf* e *ovwdb.lrf*).

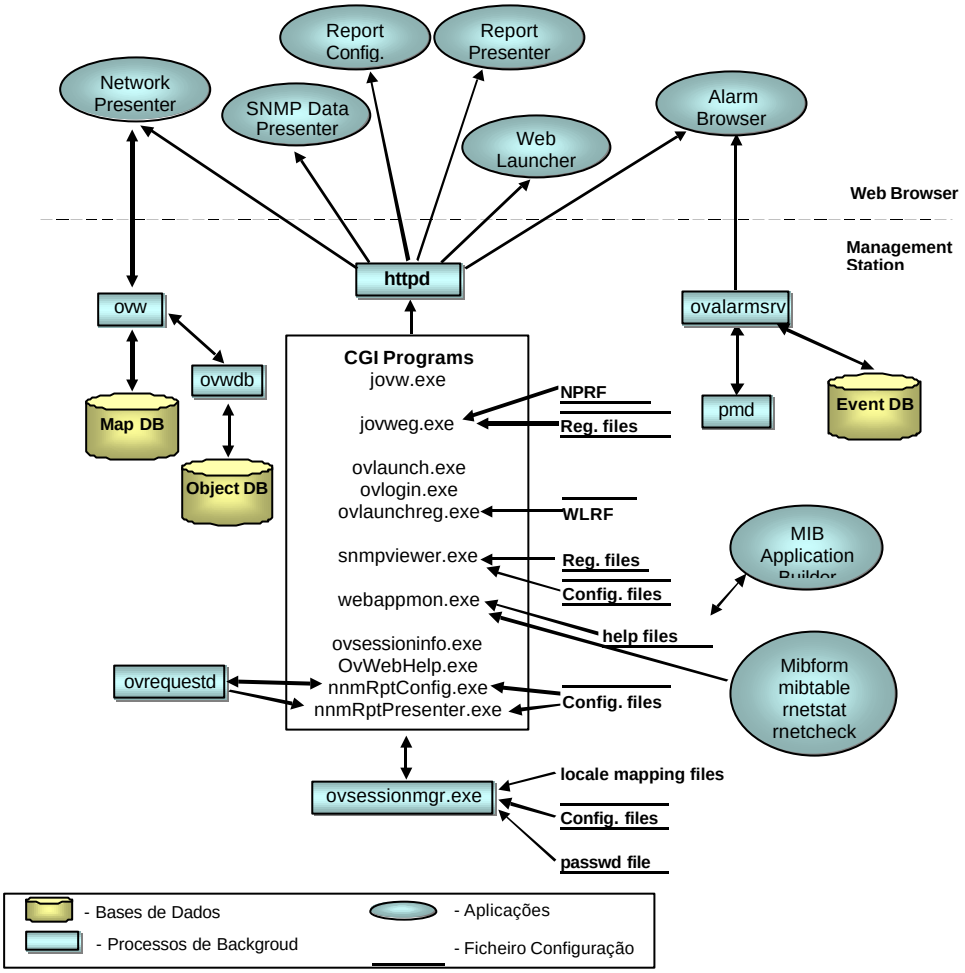


Figura 4.31 – Funcionamento dos módulos da interface Web.

4.4.1.9 Ferramentas Disponíveis

No que respeita à operação, as funções do NNM são auxilidas por um conjunto de ferramentas que facilitam a execução das várias tarefas de administração, podendo ser encontradas tanto nos menus da aplicação de gestão como na interface WEB. Estas ferramentas podem ser agrupadas em quatro grupos distintos, sendo eles a análise de desempenho, configuração, análise de falhas e ainda um grupo de ferramentas diversas.

No respeitante à análise de desempenho, o NNM disponibiliza ferramentas que permitem observar, em tempo real, informação sobre: as interfaces (o estado, o tráfego, os erros,...); as variáveis do sistema (espaço em disco, memória, carga do processador, as ligações TCP estabelecidas, ...); o desempenho da estação gestora, sobre o tráfego SNMP, etc.

As ferramentas de configuração permitem efectuar uma análise rápida da configuração e das características dos objectos, sendo possível obter de uma forma simples e directa informação sobre as propriedades das interfaces, os endereços IP atribuídos, as tabelas de encaminhamento, as tabelas de ARP, a configuração do parâmetros do SNMP, os serviços activos e diversa informação sobre o sistema.

Na área da análise e resolução de falhas encontram-se módulos que possibilitam a rápida identificação de um problema, quer pela análise de eventos passados quer pelo teste dos objectos em tempo real. Estes módulos permitem para um determinado objecto ou conjunto de objectos, visualizar os alarmes recebidos, testar o estado de todas as suas variáveis, identificar rapidamente as suas propriedades, testar a conectividade entre dois nós remotos (possível quando um dos equipamentos possui um agente SNMP EMANATE), testar o funcionamento dos protocolos IP/TCP/SNMP, entre outras funcionalidades.

No capítulo das ferramentas diversas encontram-se vários utilitários que potenciam uma maior flexibilidade da plataforma, sendo exemplo disso o browser para visualização de MIBs, um browser para visualização de objectos DMI, acesso rápido a consolas de telnet, activação remota de sistemas, ferramentas para exportação de dados.

4.4.1.10 Considerações Sobre a Configuração do NNM

Antes de dar início à instalação e colocação em funcionamento do NNM é necessário proceder a alguma planificação de modo a tirar o máximo rendimento da plataforma. Neste processo foram tidas em conta as referências [NNM00i] e [NNM00j]. Assim, existem alguns pontos que convém acautelar à partida, entre eles:

- Criar procedimentos para cópias de segurança;
- Definir e configurar o tempo de *polling* para os vários objectos;
- Identificar quais os objectos que vão ser geridos e quais não vão e criar os filtros de acordo;
- Definir os objectivos do sistema de monitorização de eventos e implementá-lo em consonância;
- Definir as variáveis que irão ser monitorizadas e configurar o colector de dados estatísticos de forma a responder às necessidades;
- Configurar os mapas de acordo com as necessidades de gestão;
- Definir planos de manutenção do NNM;

Depois de acauteladas estas questões poderá passar-se à instalação da plataforma, tendo em conta que, a estes factores, deve acrescentar-se a correcta configuração dos parâmetros de rede dos diversos equipamentos, para que o NNM identifique correctamente os objectos e a sua interligação. Esta configuração dos parâmetros passa pela definição e implementação de um esquema de endereçamento IP consistente, pela correcta atribuição das máscaras de sub-rede, pela definição de blocos de IP atribuídos pelo DHCP, pela correcta configuração do sistema de DNS, pela implementação de agentes SNMP nos equipamentos e sua correcta configuração; em suma, o correcto funcionamento do NNM irá depender, em grande parte, da correcta configuração da infra-estrutura e da ausência de erros procedimentais na constituição desta.

4.4.2 Transcend Enterprise Manager NT

Os fabricantes de equipamentos de rede possuem, normalmente, aplicações de gestão próprias que permitem tirar partido de todas as funcionalidades dos seus equipamentos. O NNM, como já foi referido, por si só, não pretende substituir as aplicações de gestão específicas desses fabricantes, mas visa antes a constituição de uma plataforma base, na qual poderão ser integradas aplicações de terceiros. Esta facilidade de integração é uma das chaves para o sucesso do NNM e é exactamente neste cenário que o Transcend Enterprise Manager (TEM) se enquadra.

Atendendo ao facto da maioria do equipamento de rede (do tipo concentrador ou comutador Ethernet), na infra-estrutura de comunicações da Universidade de Aveiro, ser da marca 3COM optou-se pela adopção do TEM, como sendo uma aplicação que traria mais valias na gestão dos equipamentos desta marca.

O TEM é uma aplicação que se destina a efectuar operações de gestão sobre toda a panóplia de equipamentos da 3COM. No entanto, a infra-estrutura sobre a qual vai ser implementada a plataforma de gestão possui apenas alguns tipos de equipamentos, pelo que o TEM foi estudado na mesma dimensão, razão pela qual a descrição que se fará de seguida das várias funcionalidades do TEM será apenas extensiva onde se justifique para o presente trabalho.

4.4.2.1 Central de Gestão e Inventário

A Central de Gestão efectua a interligação entre a base de dados do NNM e a base de dados do TEM disponibilizando neste último uma interface de gestão da base de dados interna, suportada por *Sybase SQL Anywhere*.

Através desta interface é possível importar todos os objectos 3COM do NNM e organizá-los por grupos de modo a reflectirem a organização da empresa, tendo associado um conjunto de funcionalidades que passam pela organização gráfica dos equipamentos de rede consoante o tipo e a localização, pela facilidade de alteração da disposição dos objectos, pelos menus de acesso rápido às restantes ferramentas do TEM e pela geração de relatórios dos equipamentos e suas características [TEM97a].

A Figura 4.32 mostra a interface disponibilizada pela central de gestão, onde podem ser observados os equipamentos agrupados, as características do equipamento seleccionado e um conjunto de dados disponibilizados pelas ferramentas acessíveis através da Central de Gestão.

A informação da Central de Gestão encontra-se armazenada numa base de dados suportada pelo *SQL Anywhere*, existindo uma série de operações de manutenção que devem ser efectuadas sobre aquela e que são inerentes ao *SQL Anywhere*, pelo que não serão abordadas neste trabalho.

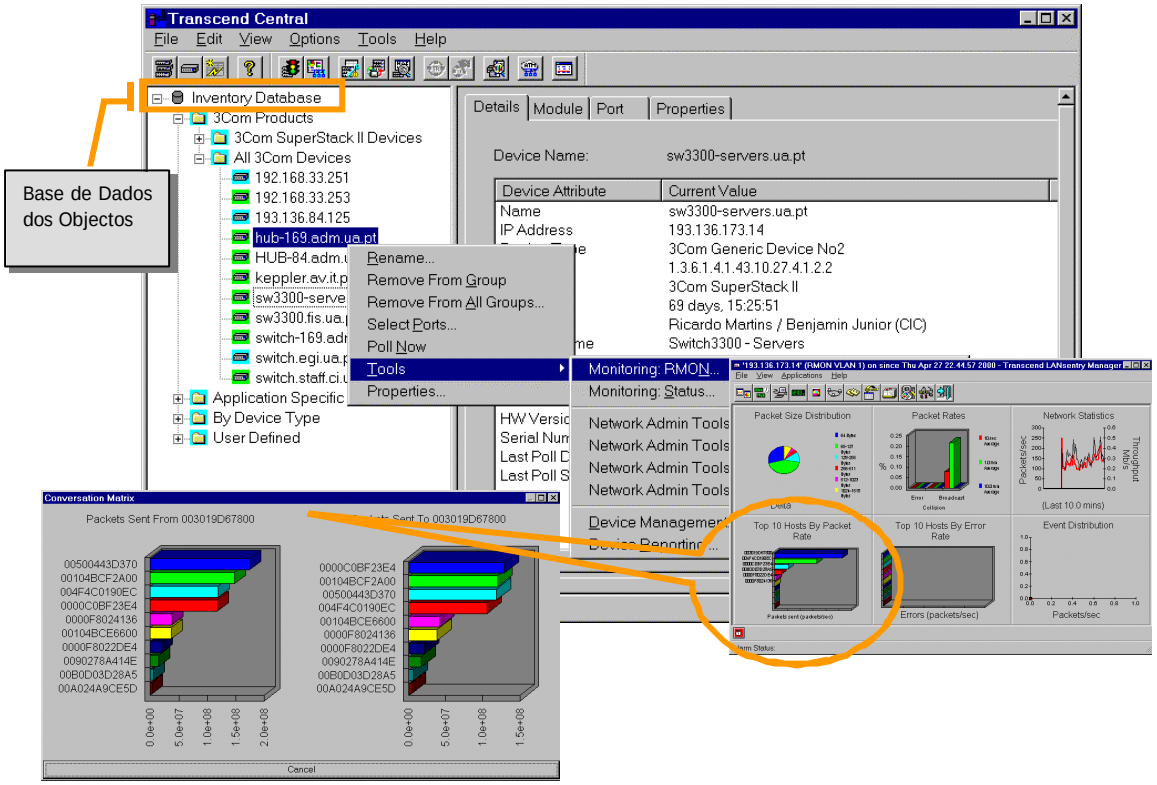


Figura 4.32 – Interface da central de gestão do TEM.

A partir desta interface é possível gerar um conjunto de relatórios que possibilitam ter um inventário sempre actualizado dos equipamentos existentes na rede, dos módulos que os constituem e das configurações de cada um.

4.4.2.2 Gestão e Estatísticas de Equipamentos

Uma das ferramentas acessíveis através da Central, ou directamente a partir do NNM, é a interface *Device View* (Figura 4.33). Esta interface apresenta, para o equipamento em questão e baseada em SNMP, a aparência exacta do mesmo, permitindo a execução das tarefas administrativas através da interface. Os símbolos e, consequentemente, as funcionalidades disponíveis, que representam os equipamentos 3COM nos mapas do NNM, são alterados por esta aplicação, permitindo um acesso rápido às ferramentas de gestão do equipamento a partir do NNM, sendo que, para aceder às ferramentas de gestão dos equipamentos 3COM, raramente é necessário utilizar a central do TEM.

4.4.2.3 Monitorização e Análise

Os equipamentos da 3COM suportam RMON na maioria dos casos, no entanto, os grupos disponibilizados variam com o tipo de equipamento e a versão do software que estão a executar. Nesta área o TEM disponibiliza o *LANSentry Manager* que é uma aplicação para operar com agentes RMON, podendo efectuar a monitorização e análise instantânea ou histórica de um troço de rede ligado a um equipamento 3COM.

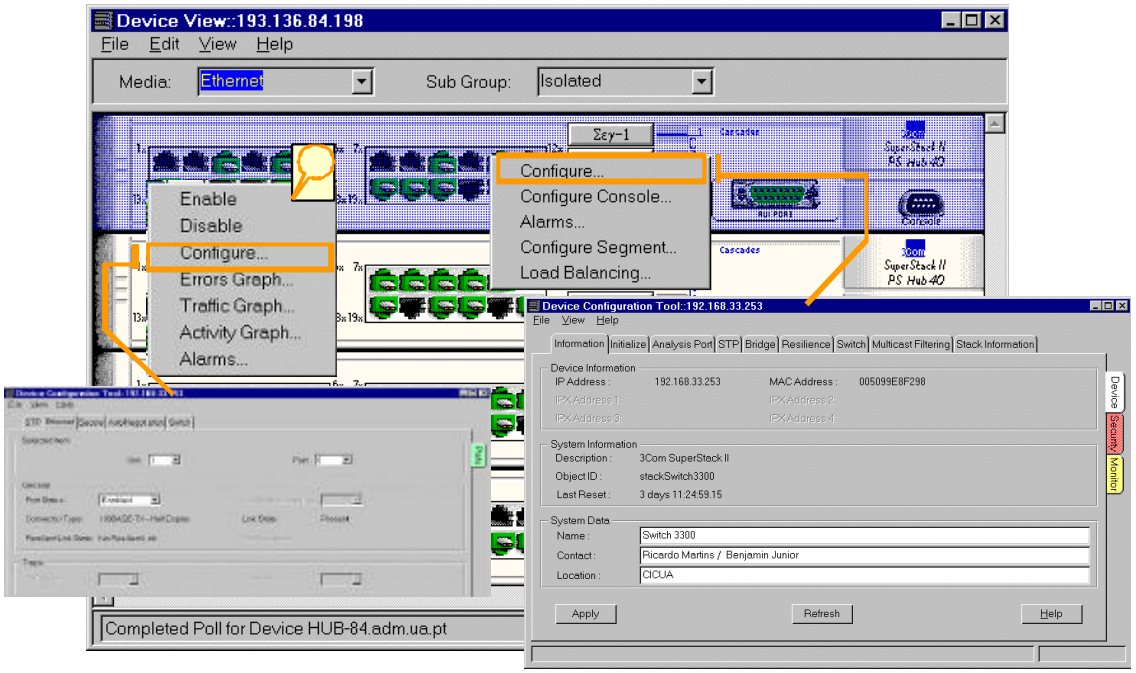


Figura 4.33 – Interface do Device View com configuração do módulo.

O *LANSentry Manager* consiste num conjunto de utilitários que permite a recolha, análise e visualização dos dados, recolhidos pelos equipamentos que implementam RMON. A taxa de utilização de um determinado troço, a ocorrência de erros nos pacotes, de colisões e de um modo abrangente o desempenho da rede, são algumas das variáveis passíveis de monitorar através do LANSentry.

Configuração

Um dos utilitários que faz parte do LANSentry, o *Config Manager*, possibilita a configuração de sondas remotas.

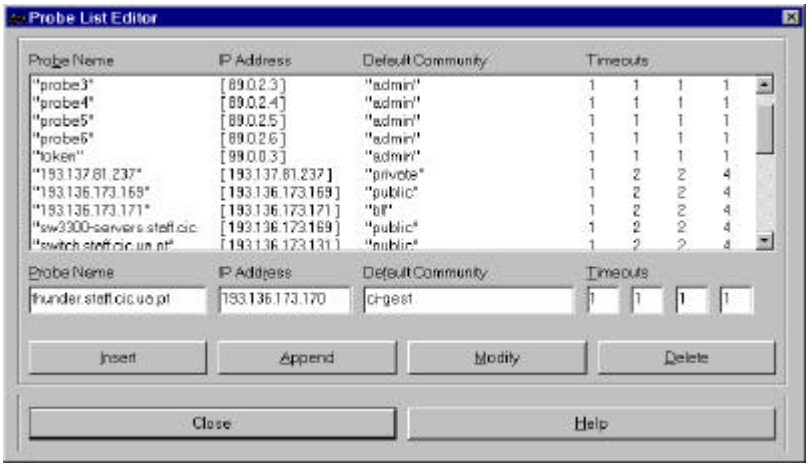


Figura 4.34 – Interface de configuração dos equipamentos 3COM.

As possibilidades de configuração vão desde a configuração da sonda até à definição de interfaces de monitorização. Algumas destas funcionalidades requerem a existência de uma sonda RMON específica, o que não se verifica no presente trabalho, pelo que apenas poderão ser testadas e abordadas as funcionalidades implementadas pelas sondas existentes nos comutadores e concentradores.

Análise em tempo real

A análise em tempo real é efectuada pelo Viewman, utilitário que mostra algumas estatísticas que possibilitam uma análise do comportamento do troço de rede, nomeadamente a distribuição do tamanho dos pacotes, a taxa de pacotes, bits e erros transmitidos, as máquinas que mais comunicam e a distribuição de eventos (colisões, erros de alinhamentos, etc.) em função da taxa de pacotes.

Esta informação é de grande relevância já que possibilita, com uma análise superficial a identificação de problemas no troço de rede onde o equipamento está inserido. A informação apresentada na Figura 4.35, não é suficiente para identificar o problema e a sua fonte, mas é indicadora do caminho que se deve seguir para com maior eficiência se chegar a esses resultados.

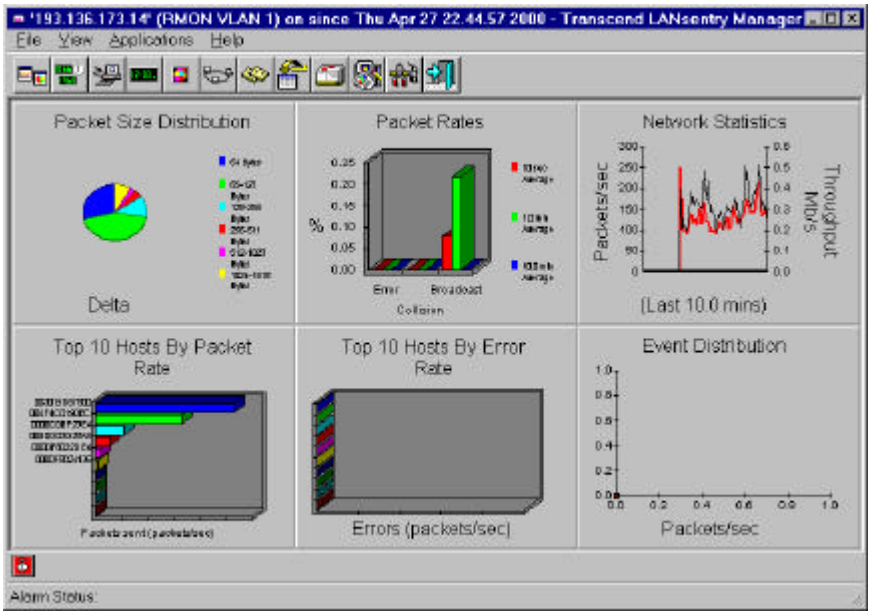


Figura 4.35 – Estatísticas globais de um troço de rede.

Nesta interface, pode ainda ser interessante a matriz de comunicação de uma máquina, acessível com um simples clique do rato (Figura 4.36) e que mostra com quem é que a máquina mantém a sua comunicação e o número de pacotes enviados e recebidos por cada estação.

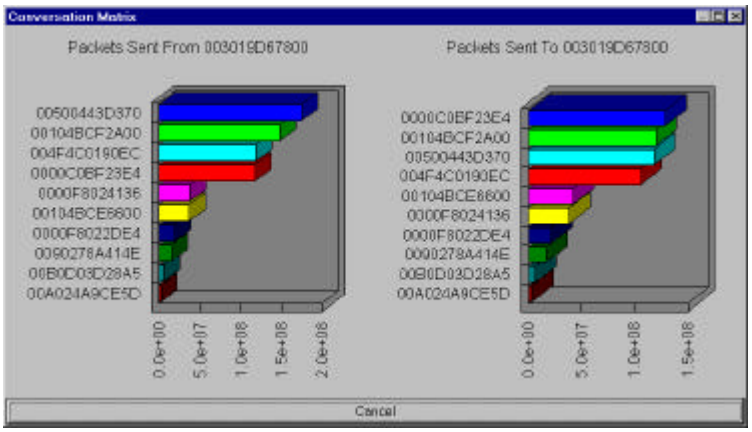


Figura 4.36 – Gráfico do tráfego de/para uma máquina.

Análise do historial

O RMONView, ao contrário do Viewman, possibilita a visualização de várias colecções simultaneamente, designadas por vistas, podendo os dados ser apresentados na forma tabular ou num gráfico que perspective o comportamento do troço de rede em análise. Esta é uma ferramenta com a maior importância na identificação do problema, já que efectua uma análise mais aprofundada do comportamento do troço de rede.

Na visualização dos grupos RMON, nos equipamentos existentes na infra-estrutura em estudo, é possível efectuar a monitorização das seguintes vistas:

- Estatística;
- Histórico;
- Nó;
- Matriz;
- Alarmes;

Cada uma destas vistas pode ser configurada em termos de variáveis a ser recolhidas, intervalos de tempo e sondas que as irão disponibilizar.

A estatística apresenta um relatório em tempo real da actividade de um troço de rede e deverá ser a primeira vista observada quando se suspeite de problemas na rede. O histórico é um complemento da estatística permitindo a recolha de dados acerca do comportamento da rede ao longo do tempo e cuja análise permitirá estabelecer limites de aviso que denunciem eventuais anomalias na rede e as permitam prevenir. A vista dos nós recolhe, para cada nó, uma série de estatísticas que permitem, na globalidade da rede, identificar possíveis fontes de problemas. A matriz regista os valores estatísticos da comunicação entre um par de nós. Os alarmes podem ser configurados com o objectivo de avisar o gestor de que uma variável ultrapassou um limite predefinido, sendo estes limites impostos pelo gestor.

Geração de relatórios

Os relatórios são uma funcionalidade muitas vezes esquecida nas aplicações, mas de grande importância quando se pretende saber o "estado da arte" de uma infra-estrutura. Ora a informação, relativa a todos os equipamentos, está na base de dados das aplicações; o que por vezes falta são ferramentas que extraiam esses dados e, de uma forma inteligível, os apresentem ao gestor.

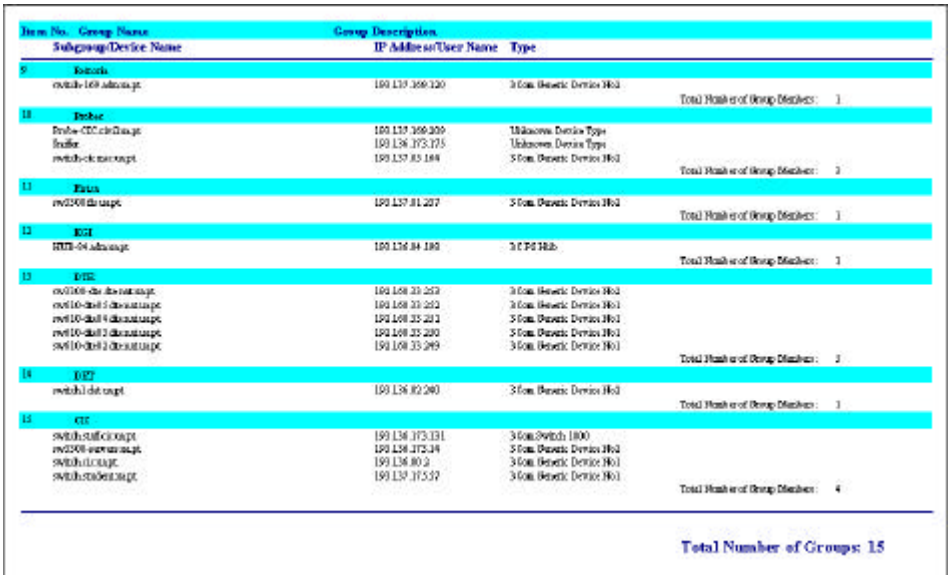


Figura 4.37 – Relatório gerado pelo TEM.

No caso do TEM, são disponibilizados relatórios com informação sobre a quantidade, localização e características de hardware e software dos equipamentos (Figura 4.37).

4.4.2.4 Configuração Avançada

Numa organização de grande dimensão a configuração dos equipamentos é uma das tarefas que, mesmo sendo repetitiva, requer grande concentração e cautela na sua realização. O Global Configurator do TEM realiza estas funções de um modo automático sobre um conjunto de equipamentos predefinido.

A tarefa de actualizar o software dos equipamentos é também automatizada possibilitando ao gestor saber qual a versão do software de cada equipamento e fazer a sua actualização, quer individualmente quer em grupo, reduzindo significativamente o tempo de execução destas tarefas.

O acesso a estas ferramentas pode ser efectuado a partir da Central de Gestão do TEM ou do mapa do NNM, podendo neste caso ser seleccionados os equipamentos a actualizar e posteriormente enviar a actualização para todos eles simultaneamente.

4.4.2.5 Gestão de ATM e de VLANs e de Token Ring

A utilização de ATM e de VLANs possibilitam a migração dos equipamentos de encaminhamento de nível 3 para a periferia da rede sendo a comutação efectuada no nível 2, aumentando assim o desempenho da rede [TEM97b]. A gestão de VLANs e ATM nos equipamentos 3COM é facilitada através de uma ferramenta, cuja interface gráfica mascára a complexidade da linha de comandos. No entanto, uma vez que não existiam implementações destas configurações nos equipamentos da UA, esta ferramenta não foi explorada, ficando apenas a ressalva da sua utilidade e importância na configuração de uma rede deste tipo.

As redes Token-Ring também aqui são contempladas com uma ferramenta de gestão específica mas, pelos motivos apresentados acima, a aplicação também não foi explorada ficando apenas a sua referência.

4.4.2.6 TEM Web

À semelhança do NNM, o TEM também possui uma interface Web que permite, através de um browser aceder a algumas das funções desempenhadas pela aplicação, integrando-se de com a interface Web do NNM ou podendo ser completamente autónoma (Figura 4.38).

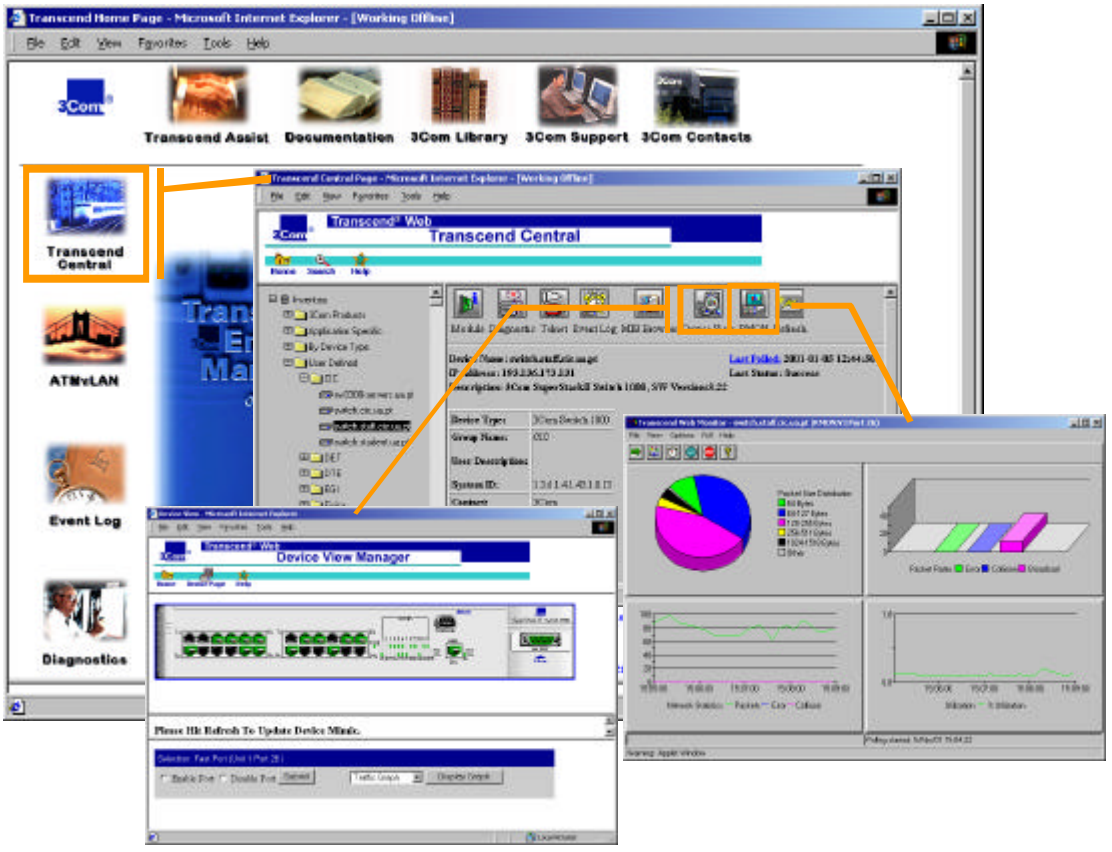


Figura 4.38 – Interface Web do TEM.

Entre as funcionalidades acessíveis através da interface Web estão a estrutura e organização dos objectos na central de gestão, a visualização das características, o acesso aos eventos de um determinado objecto recolhidos pelo NNM, e o acesso à interface *device view* disponibilizada pelo TEM e o acesso à informação estatística RMON.

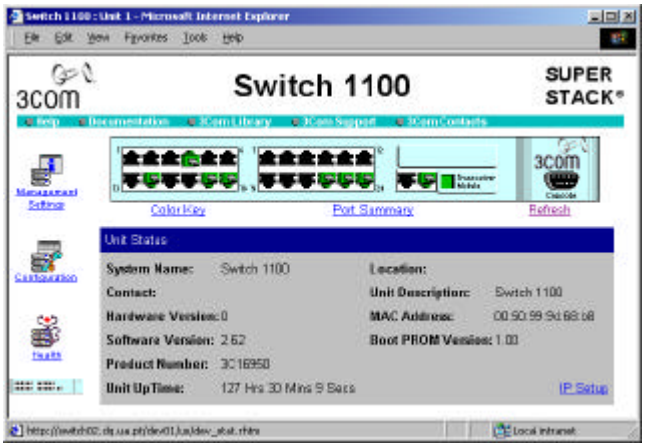


Figura 4.39 – Interface Web disponibilizada pelos equipamentos 3COM.

Os equipamentos da 3COM disponibilizam uma interface Web de monitorização e configuração que permite executar sobre eles um conjunto de funções sem a necessidade de recorrer à interface de configuração através de linha de comandos (Figura 4.39).

4.4.3 Observer Suite

Dada a importância que hoje em dia as redes têm para qualquer sector de actividade, o seu bom desempenho será uma das chaves de sucesso de qualquer deles. Para garantir o bom funcionamento das redes de comunicações é necessário identificar e compreender o tráfego que nelas circula, tráfego que é proveniente de centenas de aplicações e equipamentos e com exigências completamente diferentes.

Nesta perspectiva, e dado que a maioria das aplicações de encontra segmentada em áreas de actuação não existindo nenhuma aplicação integrada, existem vários analisadores de protocolos, que colocados num troço de rede recolhem informação sobre o tráfego desse mesmo troço. Um deles, o Distributed Observer, será o objecto de estudo nesta secção.

4.4.3.1 Funcionamento

O Distributed Observer [NIT00] é constituído por uma (ou mais) sondas em software, que pode ser instalada em qualquer ponto da rede, e por uma consola de gestão que recolhe os dados das várias sondas apresentando-os ao gestor de uma forma inteligível.

As sondas estão divididas em dois tipos, a *Advanced Probe* e a RMON *Probe*. A primeira é compatível apenas com o Observer, a segunda comporta-se como uma qualquer sonda RMON2, podendo ser acedida por qualquer aplicação de gestão RMON existente no mercado. Sendo teoricamente baixa a carga que a sonda provoca nas máquinas onde está

instalada, ela pode ser instalada em qualquer máquina com sistema operativo Windows existente na rede, bastando para isso estar licenciada. Esta condição não se observou na implementação prática efectuada, sendo os recursos do sistema completamente ocupados com a sonda em funcionamento. No entanto, para facilitar a sua utilização, a sonda pode ser instalada em modo aplicação ou em modo serviço (nos sistemas Windows NT), com uma interface onde o gestor pode configurar o seu arranque automático e funcionamento autónomo.

4.4.3.2 Consola de Gestão Observer

O Observer reúne numa mesma interface um conjunto de ferramentas que efectuam a análise aos vários tipos de parâmetros da rede (Figura 4.40). Nesta panóplia de ferramentas, algumas só podem ser usadas com as sondas *Advanced Probe*, ao passo que outras são usadas também para analisar sondas RMON.

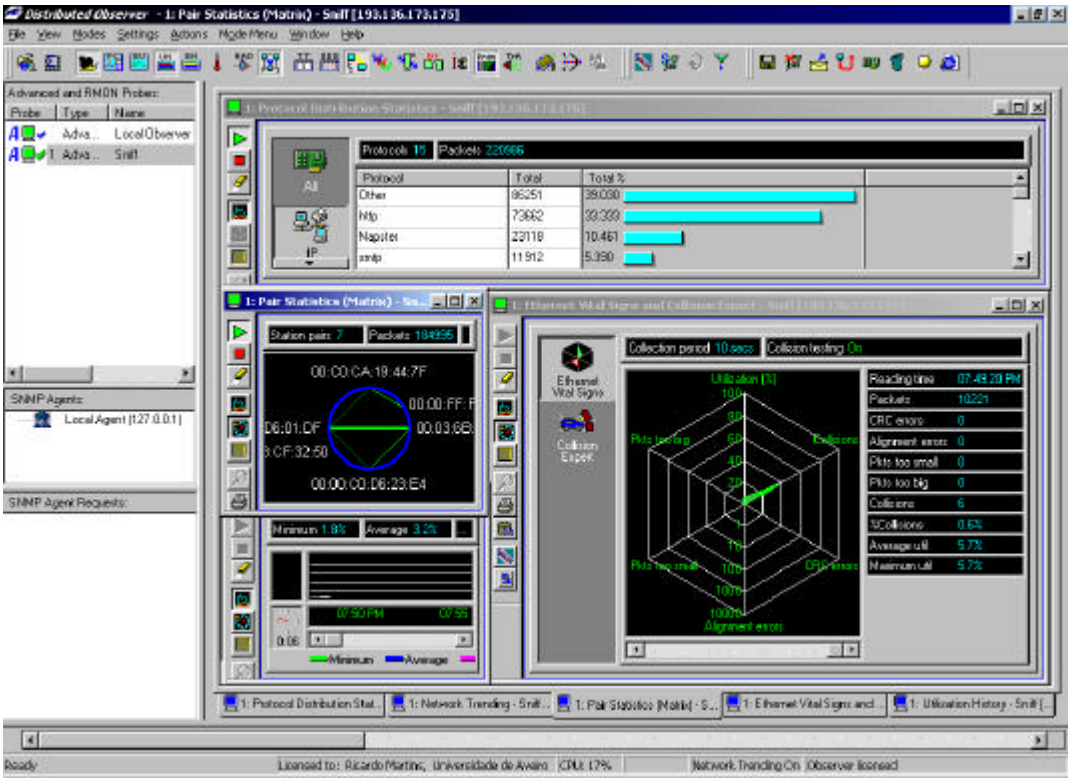


Figura 4.40 – Interface do Observer.

4.4.3.3 Sondas

Os dados são recolhidos por sondas distribuídas pela rede que depois os enviam para o Observer. Existem dois tipos de sondas, que podem ser instaladas em qualquer sistema Windows 9.x/NT/2000:

- **RMON Probe** – é uma sonda RMON compatível com as normas RMON1/2.

- **Advanced Probe** – é uma sonda com um conjunto de funcionalidades adicionais à sonda RMON e que permite recolher o historial da rede mesmo sem estar ligada ao Observer.

4.4.3.4 Extensões

As extensões acrescentam funcionalidades de análise ao Observer, podendo ser adquiridas separadamente consoante o tipo de gestão que se pretende efectuar. A versão 7 do Observer inclui as seguintes:

- **Expert Extension** – Esta extensão providencia mecanismos de captura e análise de pacotes em tempo real, com a identificação de uma série de parâmetros relativos à comunicação num troço ou à comunicação entre duas máquinas específicas.
- **RMON Extension** – Processa a informação RMON recolhida das sondas, apresentando-a numa interface intuitiva e simples de analisar.
- **SNMP Extension** – Disponibiliza um conjunto de funcionalidades que permitem recolher e analisar informação de um agente SNMP.
- **Web Extension** – Disponibiliza os dados recolhidos pelo Observer numa interface Web, permitindo que vários clientes tenham acesso à informação.

4.4.3.5 Captura e Descodificação de Pacotes

Para efectuar uma análise mais profunda do tráfego que circula na rede, o Observer permite capturar e descodificar pacotes de vários protocolos, incluindo: TCP/IP, SNMP, NetBios/NetBEUI, IPX/SPX, AppleTalk e SNA.

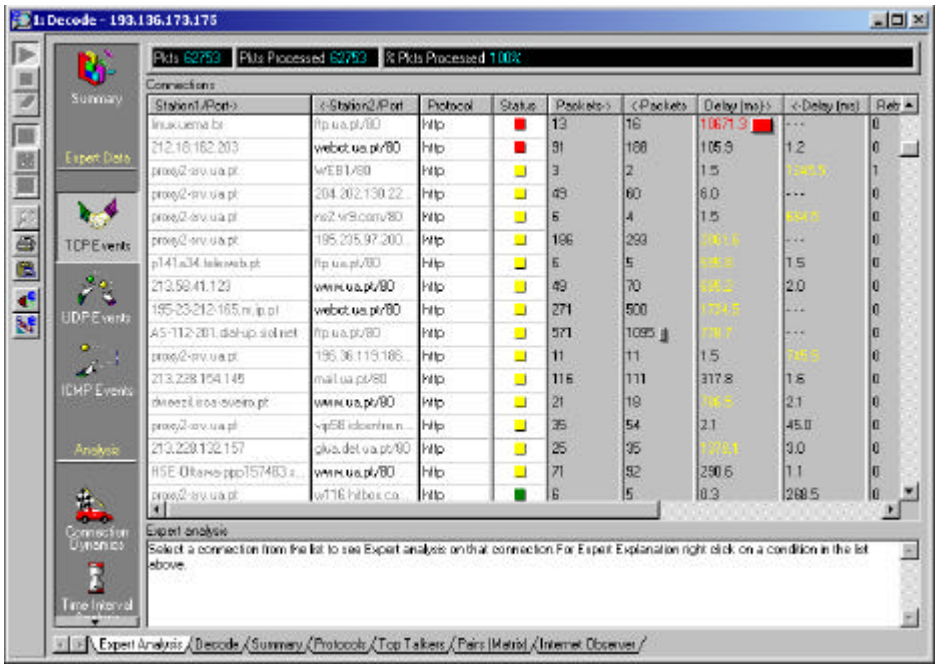


Figura 4.41 – Opções de análise do Observer.

A captura pode ser limitada através de filtros que incluem ou excluem: pacotes, estações, erros, etc. As opções de análise disponibilizadas pelo Observer vão desde a análise do tipo de pacotes e tráfego até ao tempo de resposta das aplicações e sessões estabelecidas, incluindo uma análise dinâmica da ligação com medição de todos os tempos entre pacotes trocados.

4.4.3.6 Estatísticas em Tempo Real

Na análise do comportamento de um troço de rede existem algumas variáveis que devem ser medidas em tempo real, de modo a evidenciar problemas que serão analisados com mais pormenor com outras ferramentas, concretamente:

- **Utilização da Largura de Banda**;
- "**Top Talkers**" (Análise das estações que mais dialogam, com quem dialogam e que protocolos usam);
- **Distribuição de Protocolos**;
- **Estatísticas de pares – Matriz** (Estações que mais dialogam entre si);
- **Analisador de Internet** (Analisa quais os utilizadores, que recursos ocupam no acesso à Internet, onde acedem e quais os protocolos que usam).

4.4.3.7 Interface WEB

A interface WEB providência o acesso aos dados estatísticos disponíveis no Observer (Figura 4.42).

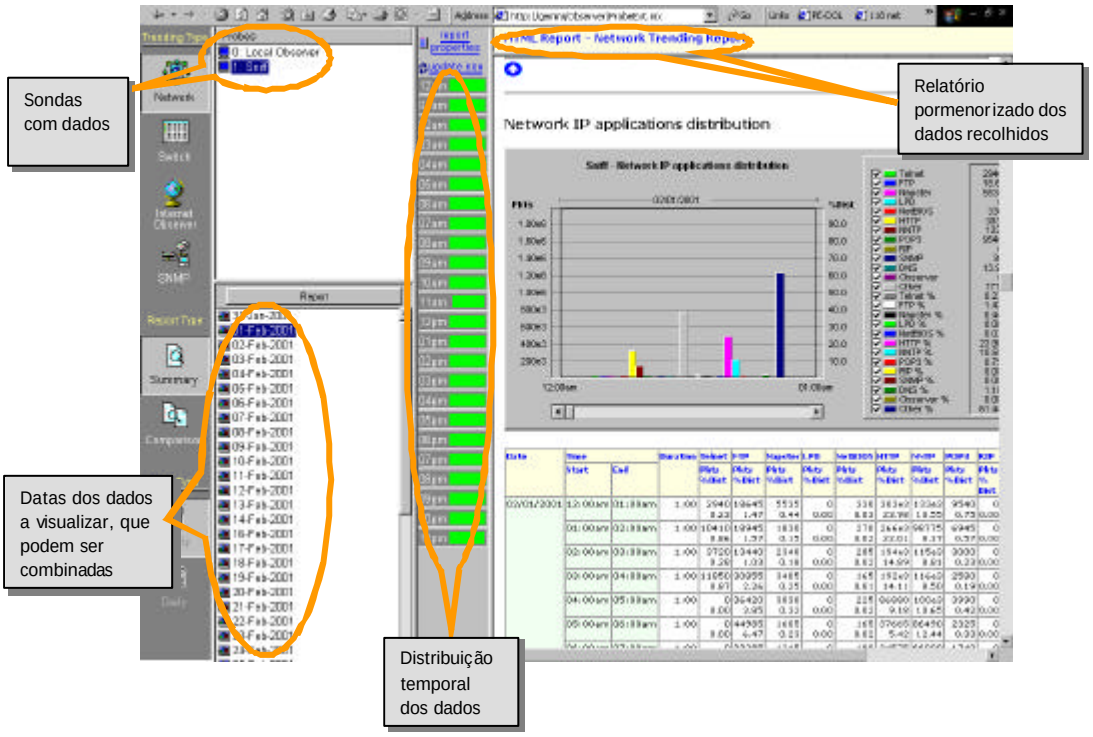


Figura 4.42 – Interface Web do Observer.

Esta interface proporciona o mesmo tipo de informação, que a aplicação Observer, com a vantagem de ser acedida através de um browser Web disponibilizando em tempo real e de um modo configurável pelo utilizador, toda a informação recolhida pelas sondas activas e configuradas no Observer.

4.4.3.8 Rasteio de Erros

A origem dos erros é, na sua maioria, um dos pontos de difícil detecção no diagnóstico de problemas numa rede de dados, pelo que ferramentas que possam identificar os equipamentos com problemas são de grande utilidade. Nesta área, o Observer disponibiliza dois utilitários, um deles que recolhe e apresenta os sinais vitais da rede, como tamanho dos pacotes, CRC, colisões e alinhamento, o outro que recolhe dados relativos a erros diferenciando-os por estação.

4.4.3.9 Análise do Historial

Tal como já foi referido ao longo do trabalho, a análise do historial do comportamento da rede é um dos pontos essenciais para poder efectuar um planeamento concertado. O *Network Trending* é uma ferramenta que permite recolher e armazenar ao longo do tempo os dados do comportamento do troço e da comunicação estabelecida entre equipamentos.

4.4.4 Systems Management Server

De entre a panóplia de plataformas de gestão de sistemas existentes no mercado, neste ponto será destacado o SMS. O SMS é uma das plataformas que, pelas suas características, se adapta perfeitamente a qualquer infra-estrutura, apresentando uma estrutura modular e escalável, podendo gerir redes com algumas dezenas de PCs, até redes com vários milhares de equipamentos, possuindo preços muito aliciantes para as instituições de ensino.

4.4.4.1 Organização em Sítios

A arquitectura modular do SMS baseia-se na atribuição de papéis, que podem ser protagonizados por diferentes equipamentos e organizados numa estrutura hierárquica. A organização dos sítios, hierarquicamente, sustém a base para a escalabilidade anunciada pelo SMS, agrupando os equipamentos em subdivisões, que se podem adaptar tanto à estrutura física como lógica da infra-estrutura (Figura 4.43).

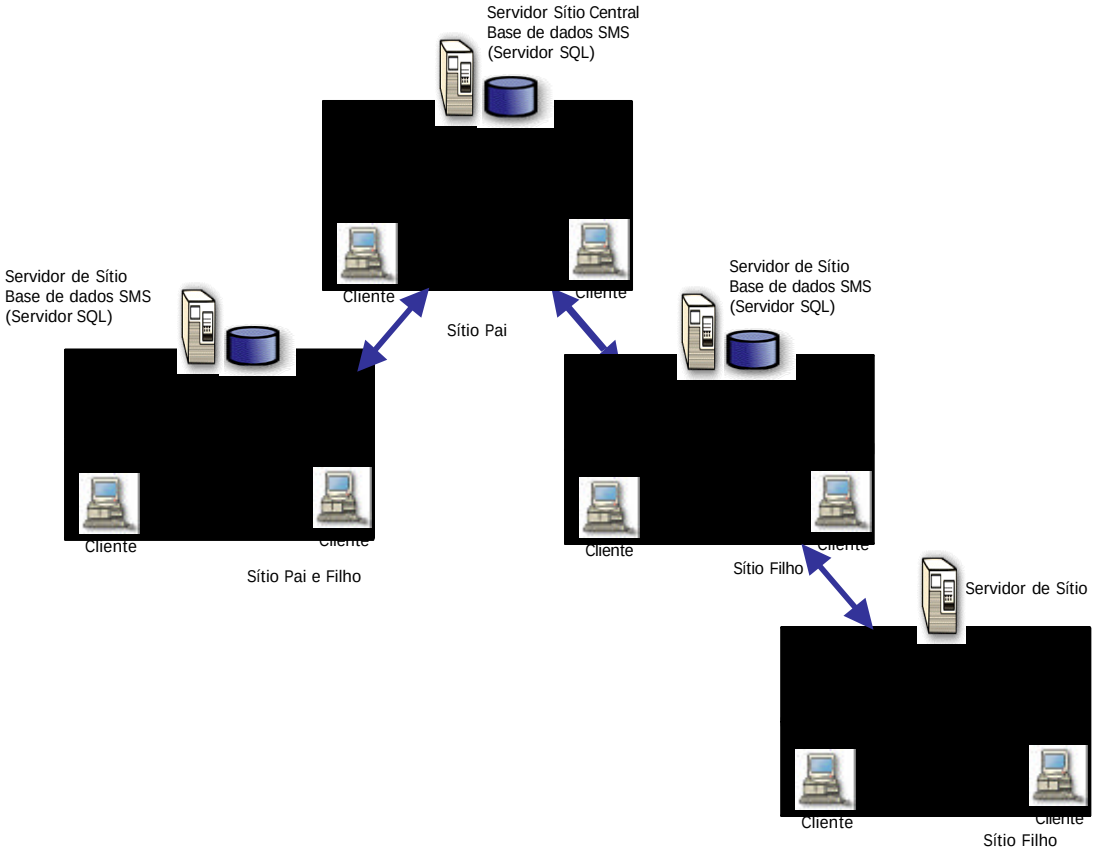


Figura 4.43 – Organização hierárquica do SMS.

A cada sítio está associado um conjunto de papeis que podem ser distribuídos quase que individualmente por cada máquina integrante do sítio. Dos papéis que poderão ser desempenhados em cada sítio, destacam-se:

- **Cliente Access Point (CAP)** – funciona como ponto de comunicação entre os clientes e o servidor do sítio, providenciando um mecanismo de redução de carga neste e desempenhando as funções de colecção e difusão de informação de e para os clientes.
- **Distribution Point (DP)** – Armazena e providência para os clientes, os pacotes de software que se pretendem instalar. Depois dos clientes receberem uma notificação através do CAP, o DP é contactado no sentido de fornecer o novo software disponível.
- **Logon Point** – é o responsável pelo contacto inicial com os clientes, podendo ser utilizado para a descoberta e instalação dos clientes. Funcionando através de login scripts, este papel pode ser atribuído a servidores NT ou Novell.
- **SMS Site Database Server** – é o papel desempenhado pela máquina que suporta a base de dados do SMS, em SQL, pelo que necessitará do Servidor SQL instalado.
- **SMS Provider** – fornece a interface entre a consola de administração e o servidor contendo a base de dados.
- **Software Metering Server** – é o responsável pela gestão do controlo de licenças de software e pela comunicação com os respectivos agentes nos clientes.
- **Software Metering Database Server** – o SMS implementa duas bases de dados, uma delas para a informação geral e outra especificamente para o controlo de licenças, sendo este papel desempenhado pelo servidor que suporta a base de dados de controlo de licenças.

4.4.4.2 Arquitectura do SMS

Na arquitectura do SMS podem ser diferenciadas duas entidades, os clientes e os servidores. Começando por estes últimos, a sua arquitectura pode ser dividida em duas partes, os componentes SMS e as bases de dados (Figura 4.44) [MSC01a].

Os componentes são tarefas (*threads*), serviços e aplicações que, depois de dada alguma ordem através da consola, se encarregam de executar todos os passos para que a operação seja realizada com sucesso, quer seja ela inventário, distribuição ou contabilização de software, ou qualquer outra operação desencadeada pelo gestor.

Os componentes instalados em cada sítio dependem do conjunto de funções realizadas e podem ser instalados ou desinstalados em qualquer altura. Os dados processados são armazenados e agrupados pelo seu tipo, tal como ilustrado na Figura 4.44.

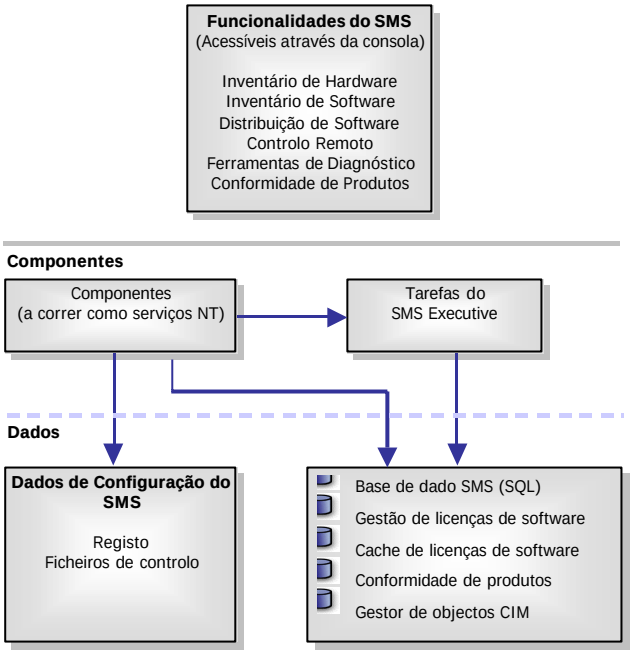


Figura 4.44 – Arquitectura do SMS.

A interface WBEM corresponde à arquitectura aberta que possibilita a criação de aplicações e scripts que poderão automatizar alguns processos de acordo com as necessidades. A criação desta interface é potenciada pelo SMS Toolkit, que providencia uma API de desenvolvimento que utiliza o WBEM para aceder à informação (Figura 4.45).

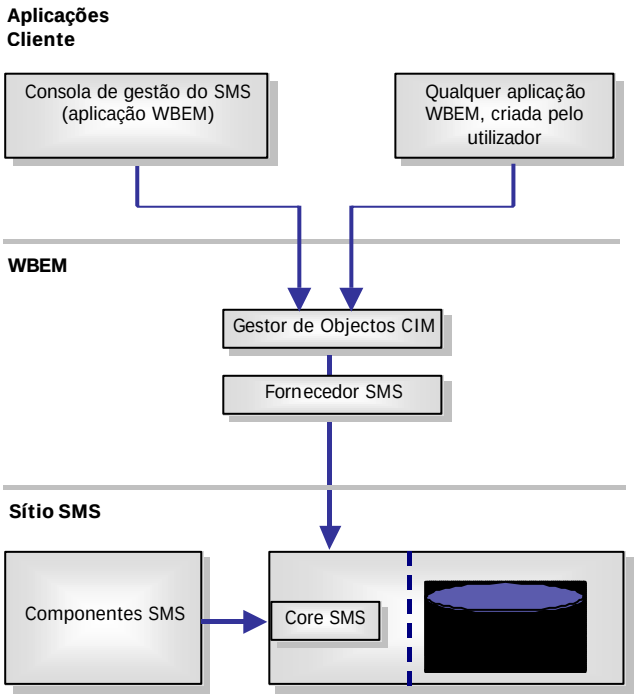


Figura 4.45 – Relação funcional entre o WBEM e o SMS.

No que respeita aos clientes, o SMS funciona baseado em serviços, que disponibilizam aos servidores de sítio os mecanismos de troca de informação. Estes serviços podem também ser variados, consoante os componentes que se pretende instalar, e são actualizados com base na configuração disponível nos CAPs.

4.4.4.3 Mecanismos de Segurança

O SMS implementa os mecanismos de segurança que controlam o acesso à informação das suas bases de dados, utilizando as facilidades disponibilizadas pelo WBEM (Figura 4.46).

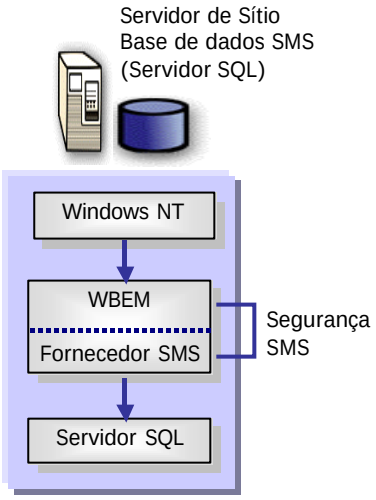


Figura 4.46 - Níveis de Segurança do SMS.

A segurança é implementada utilizando contas de utilizadores e de grupos existentes ao nível do sistema operativo, para dar direitos nos objectos e nas colecções existentes na base de dados. Para além deste existe um outro nível de segurança efectuado pelo próprio servidor SQL [MSC01b].

A instalação do SMS e o diálogo com os restantes servidores, sítios e clientes requer a configuração de um conjunto de contas específicas para esses fins, que assegurarão e limitarão o acesso exclusivo aos respectivos recursos [MSC01b]. Estes mecanismos permitem um maior controlo sobre o tipo de acesso à informação. No entanto convém estabelecer uma boa relação no binómio segurança/facilidade de gestão, de forma a facilitar as tarefas de gestão sem comprometer a segurança e integridade da informação.

4.4.4.4 Instalação dos Clientes e Descoberta de Recursos

A instalação dos clientes e a descoberta dos recursos da rede podem ser efectuadas por diferentes métodos, adequando-se estes ao ambiente onde vai ser instalado o sistema de gestão. Os métodos disponíveis permitem um maior ou menor controlo do processo de instalação e descoberta da rede, controlando deste modo o tráfego gerado pelas operações de gestão, havendo sempre uma interdependência entre os métodos de descoberta e de instalação.

Os métodos de descoberta e instalação disponibilizados pelo SMS são os seguintes:

- **Logon Discovery** – Este método é usado na descoberta de computadores, sendo inicializado através dos scripts de logon, ou através do assistente de instalação do SMS. Este método faz par com o método de instalação do mesmo nome, pelo que as alterações num deles são reflectidas no outro;
- **Netware NDS e Bindery** – São dois métodos utilizados na descoberta de computadores e activados através do scripts de logon em servidores Netware, fazendo par com os métodos de instalação do mesmo nome, estando mais uma vez as configurações dos métodos relacionadas;
- **Windows NT User e Group** – Estes são apenas processos de descoberta iniciados pelo SMS sobre os controladores de domínio, identificando os utilizadores e grupos do domínio;
- **Network Discovery** – Este é um método de descoberta de recursos da rede, que é desencadeado pelo SMS e identifica todos os recursos da rede incluindo computadores, concentradores, comutadores, encaminhadores. Este método é intensivo em termos de tráfego na rede, no entanto é o método mais rápido de popular o armazém de dados, utilizando o SNMP, o DHCP, os mecanismos de browsing e as chamadas Windows para descobrir a informação disponível;
- **Heartbeat Discovery** – É um método de actualização da informação dos clientes, que só está disponível depois de um computador ser cliente de um sítio SMS;
- **NT Remote Client Installation** – Este é um método de instalação que instala o cliente SMS sobre todos os recursos geridos. Uma vez activado, se os privilégios nas máquinas estiverem correctos, o SMS instala o cliente em todas as máquinas sem intervenção adicional. No entanto o processo de instalação pode ser controlado actuando sobre o domínio de gestão do sítio, ao especificar as redes lógicas IP que o constituem.

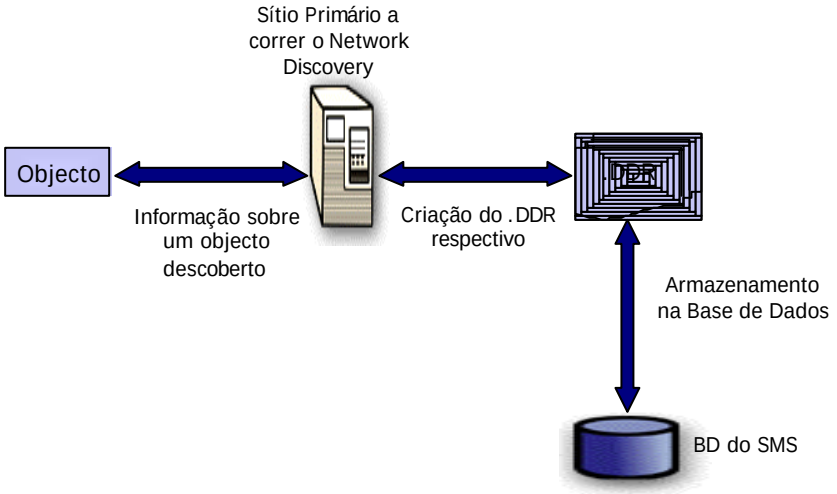


Figura 4.47 – Fluxo de informação na descoberta da rede.

No processo de descoberta da rede, sempre que é encontrado um equipamento de qualquer tipo é criada uma entrada *Discovery Data Record* (DDR) associada a esse elemento, que, depois de processada, é armazenada na base de dados do SMS, seguindo o fluxo representado na Figura 4.47.

4.4.4.5 Distribuição de Software

Uma das funcionalidades mais importantes das aplicações de gestão de sistemas é a possibilidade de, a partir de um ponto central, efectuar a distribuição de software pelos clientes. O processo de instalação de pacotes de software, baseado na filosofia de distribuição de papéis por vários sistemas, funciona como representado na Figura 4.48. Em primeiro lugar é criado o pacote de software que é enviado para o ponto de distribuição (DP), simultaneamente é enviada para o ponto de acesso de clientes, que intermedeia a comunicação entre clientes e o servidor de sítio, uma notificação sobre a disponibilização do software e da sua localização. Finalmente os clientes contactam o DP para instalarem o pacote disponível, sendo gerados relatórios individuais de cada instalação. O processo de distribuição de software é em tudo semelhante ao processo de instalação remota de clientes.

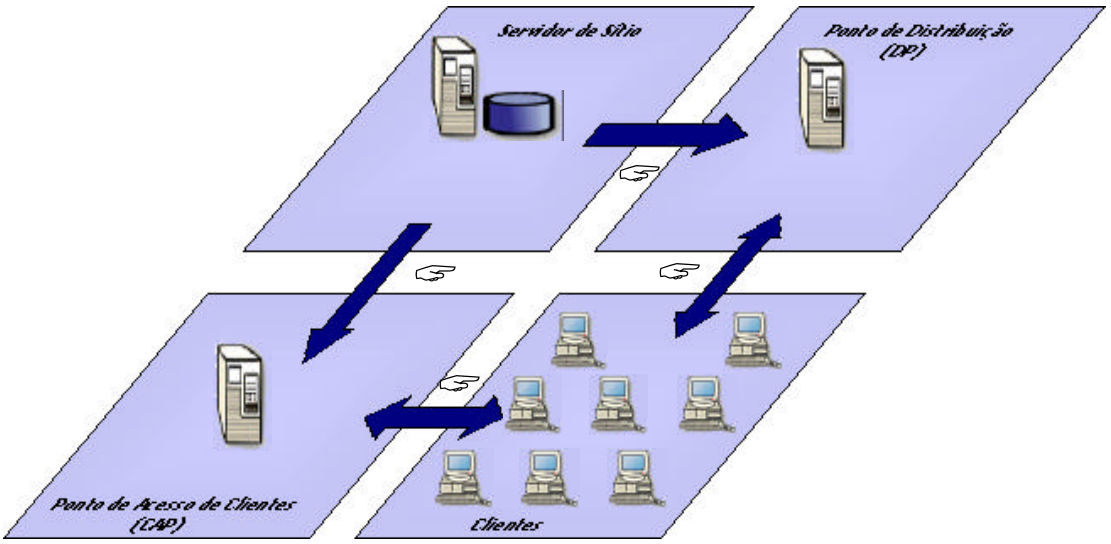


Figura 4.48 – Processo de distribuição de pacotes de software.

Os pacotes de software podem ser criados utilizando ferramentas como o *Veritas WinInstall LE [*VER00] e o *Microsoft SMS Installer* [MSC97a], que reúnem a informação necessária à instalação de um determinado software com base na monitorização das diferenças do sistema entre o pré e o pós instalação, na identificação dos ficheiros utilizados pela aplicação e na monitorização do processo de instalação. Estas ferramentas criam pacotes e scripts de instalação que podem ser configuradas, adaptando-as a um ambiente de utilização concreto.

4.4.4.6 Controlo de Licenças

O SMS pode gerir e controlar a utilização de licenças de software numa organização, funcionando através de um conjunto de processos que, distribuídos pelos clientes e pelo servidor de sítio do SMS, interagem entre si de modo a manterem uma base de dados, com informação sobre as licenças em uso, sempre acessível e actualizada.

O controlo de licenças pode funcionar em modo passivo quando o objectivo é meramente informativo ou estatístico do software usado, ou em modo activo quando se pretende um controlo efectivo das licenças em uso. Neste caso, podem ser atribuídas permissões de utilização baseadas em grupos ou utilizadores, que visem limitar o acesso a determinadas aplicações.

Este componente do SMS utiliza uma base de dados própria, separada da do SMS, funcionando também sobre SQL.

4.4.4.7 Geração de Relatórios

A informação de gestão do SMS é armazenada numa base de dados SQL, sendo acessível a partir de ferramentas como o *Access*, o *Excel*, o *Crystal Reports*, a consola de administração, etc. No entanto, todas estas ferramentas utilizam o WBEM como mecanismo de acesso à informação, concretamente o driver ODBC WBEM, que é o utilizado pelo SMS no processamento da informação. A linguagem utilizada para o acesso à informação é derivada do *American National Standards Institute Structured Query Language* (ANSI SQL), e tem por nome *WMI Query Language* (WQL), diferindo da primeira pelo facto de retornar dados de classes, em vez de tabelas, e de instâncias, em vez de linhas [MSC99c].

4.4.4.8 Monitorização da Rede

Depois de identificar os recursos da rede, o SMS permite a visualização esquemática dos sítios, incluindo os seus servidores e papéis associados. Nesse esquema encontram-se também representados os encaminhadores, existentes na interligação dos servidores e os sítios, que fazem parte da hierarquia do SMS.

Em termos de monitorização, o SMS, através do *Network Monitor* (Figura 4.49), facilita a constituição de uma plataforma de monitorização distribuída, gerida a partir de uma consola central. Esta monitorização remota pode ser feita através da instalação do Network Monitor em sistemas Windows NT/2000, que se encontrem em redes remotas e que enviam a informação para uma consola central [MSC99a].

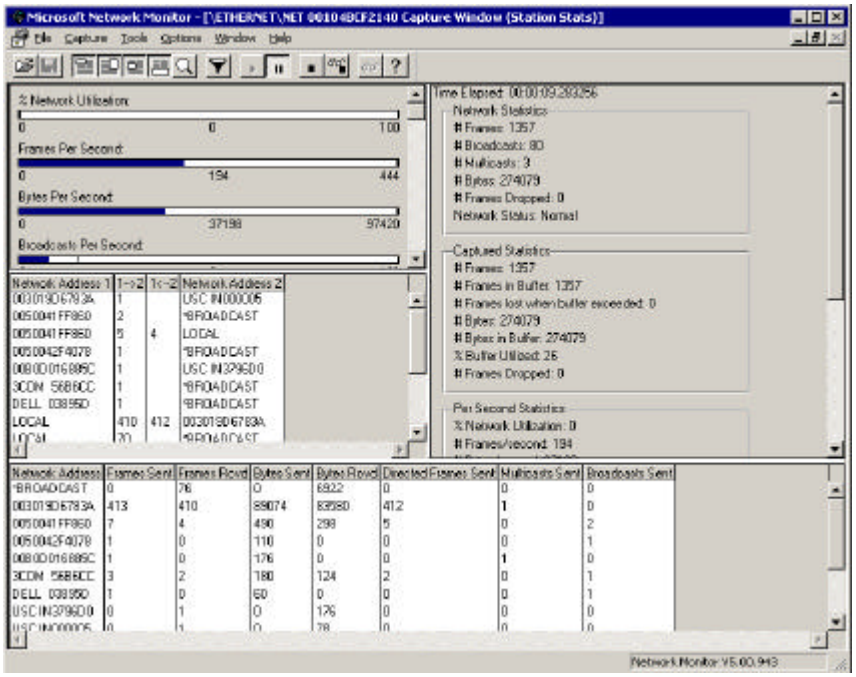


Figura 4.49 –Interface do Network Monitor.

4.4.4.9 Controlo Remoto

As ferramentas de controlo remoto são muito úteis na gestão remota de sistemas, quer porque permitem o acesso ao sistema para configuração e resolução de problemas, quer porque disponibilizam uma ferramenta de helpdesk para apoio aos utilizadores na utilização do sistema. O SMS possui uma ferramenta que, integrada com o agente SMS, disponibiliza um módulo cliente/servidor para o acesso remoto a sistemas. Esta ferramenta pode ser configurada e personalizada permitindo uma grande flexibilidade na interacção com o utilizador ou com o sistema remoto.

A distribuição desta ferramenta faz-se automaticamente, através do agente SMS, e pode ser configurada para aceder ao sistema sem qualquer tipo de restrições ou então o utilizador pode definir, no seu sistema, qual o tipo de acesso que permitirá. Em termos de segurança, poderão ser definidos, para cada colecção, os utilizadores ou grupos que terão acesso a esta ferramenta, comportamento verificado na maioria das ferramentas do SMS.

4.4.4.10 Registo de Eventos e Notificações

A análise dos eventos e notificações ocorridos com os vários componentes da plataforma é essencial tanto no planeamento de alterações, como na resolução de problemas. Neste campo, o SMS possui um sistema de eventos próprio muito completo, discriminando os eventos por componente e com facilidades de pesquisa configuráveis (Figura 4.50). A organização dos eventos revela-se muito útil e funcional.

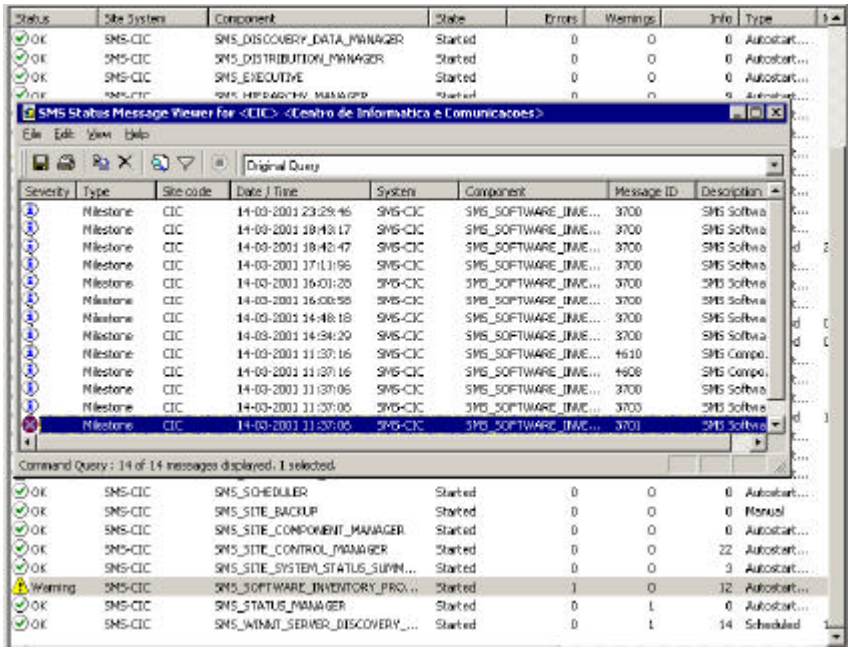


Figura 4.50 – Janela de eventos do SMS.

4.4.5 Outras Aplicações

Como complemento das aplicações comerciais, referidas anteriormente, serão utilizadas sempre que possível aplicações de domínio público que de um modo integrado ou não estendam as capacidades e funcionalidades da plataforma. Entre elas encontram-se o MRTG, para disponibilizar a informação estatística através de uma interface Web, o BigBrother para monitorização dos serviços existentes nos sistemas e o SNMP4tPC que possibilitará o acesso a contadores e variáveis, de extrema importância na monitorização de sistemas Windows.

4.5 Planeamento da Configuração

No processo de planeamento da instalação e configuração da plataforma, e depois do levantamento inicial de necessidades, atendeu-se a um conjunto de factores que terão a ver, essencialmente, com os requisitos de gestão da infra-estrutura de informática da UA, destacando-se:

- Quem vai necessitar informação?
- Que tipo de informação será necessária?
- Qual a frequência de actualização da informação?
- Qual o método de acesso à plataforma de gestão?

Respondendo às várias questões, numa primeira análise, podem ser identificados três grupos com necessidades distintas, quer ao nível dos objectos a monitorar, quer ao nível da informação recolhida.

Identificando os vários grupos temos, em primeiro lugar, os responsáveis pela manutenção da rede geral, que têm como necessidades básicas a monitorização constante dos equipamentos que constituem a rede geral, o acesso a estatísticas relativas às interfaces constituintes dos equipamentos referidos, o acesso rápido a ferramentas de diagnóstico de problemas e a geração de alertas sempre que ocorram problemas nos equipamentos.

O segundo grupo que pode ser identificado, é constituído pelos gestores das unidades, cujas necessidades, passam para o domínio das redes locais e consistem em: monitorização constante do estado dos servidores e equipamentos de rede locais, o acesso a estatísticas dos mesmos, o acesso rápido a ferramentas de diagnóstico e envio de alertas mediante a ocorrência de anomalias nos equipamentos das redes locais.

Por fim temos a equipa de HelpDesk, cujas funções necessitam de mecanismos de monitorização de toda a rede e ferramentas de diagnóstico rápido.

Em observância do disposto, será necessário configurar o NNM de modo a ter vários mapas, a recolher informação estatística sobre os equipamentos, a enviar alertas sempre que ocorram eventos predefinidos e a descentralizar o acesso à estação gestora.

Para atingir o primeiro objectivo, e uma vez que o NNM descobre a totalidade da rede e apresenta-a num mesmo mapa, será necessário estudar e implementar filtros que adeqúem a informação às necessidades de cada grupo de utilizadores. Quanto aos dados estatísticos será necessário identificar quais dados é que vão ser recolhidos, de que equipamento e seguidamente configurar as colecções a efectuar. Relativamente ao sistema de alertas terá de ser configurado o sistema de eventos, interno ao NNM, de forma a desencadear os mecanismos de alerta existentes. O último ponto prende-se com a distribuição do acesso à estação de gestão. Neste caso as opções podem ser diversas passando pelo acesso via WEB, através das consolas do NNM ou através de clientes de Terminal Server.

As funções que a plataforma de gestão irá desempenhar condicionaram, como já foi referido, a escolha da mesma, tendo sido a opção por quatro aplicações comerciais: o *HP OpenView Network Node Manag*er, o *3COM Transcend Enterprise Manager*, o *Network Instruments Observer Suite* e *Microsoft Systems Management Server*.

A opção pelo sistema operativo teve em conta os sistemas suportados, cujas características económicas e de suporte satisfizessem as necessidades do CIC. Tendo sido investigado o desempenho dos vários sistemas operativos que suportavam as aplicações, concluiu-se que a melhor relação qualidade/custo apontava para um sistema baseado em Microsoft NT/2000.

As facilidades de acesso remoto à estação gestora, para além da interface WEB proporcionada pela última versão do NNM, são parte integrante dos sistemas UNIX, através de X-Windows, mas o mesmo já não acontece com os sistemas NT normais. Por esta razão, optou-se pela implementação de um sistema Windows baseado em Terminal Server que resolve este problema através da disponibilização de consolas remotas [NNM00p].

4.6 Configuração da Plataforma de Gestão de Redes

Ao longo deste ponto será abordada a estratégia utilizada na implementação da plataforma de gestão de redes, que teve como principal objectivo dotar o CIC e a sua equipa, de mecanismos de detecção de falhas, análise de dados e prevenção de problemas na infra-estrutura de comunicações da Universidade de Aveiro.

Na estratégia seguida foram tidos em conta, entre outros, a estrutura orgânica do CIC e da UA e as necessidades específicas das funções desempenhadas pelos vários membros do CIC.

4.6.1 Instalação

A correcta instalação da plataforma pode condicionar o seu funcionamento futuro, pelo que foram seguidas todas as recomendações dos fabricantes [NNM00c]. No entanto os problemas que surgiram foram múltiplos, pois a documentação fornecida pelos fabricantes não era muito clara e alguns dos passos necessários à instalação das aplicações, foram descobertos por tentativa e erro.

Antes de mais, foi criado um domínio NT, com o objectivo albergar a informação de segurança, ao qual irão pertencer os dois servidores que suportarão a aplicação de gestão de redes e de gestão de sistemas (Figura 4.51).

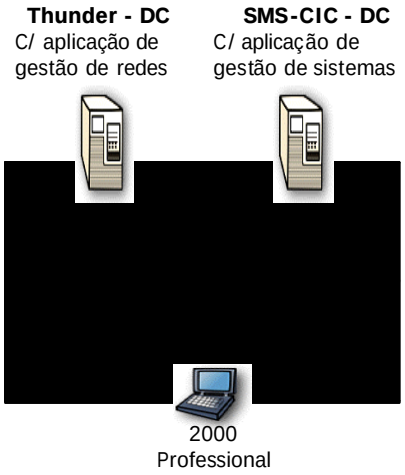


Figura 4.51 – Domínio para o sistema de gestão.

Depois de executados os trabalhos de instalação, a ordem dos passos necessários convém ser referida, sendo apresentada nos pontos seguintes.

- Instalação do SO Windows NT Terminal Server 4.0 com os seguintes componentes:
  - *Internet Information Server ;*
  - *Serviço SNMP ;*
  - *O sistema de ficheiros deve ser NTFS;*

- Instalação do Network Node Manager 6.0;
- Instalação do Transcend Enterprise Manager 97
  - *Deve ser instalada a versão completa porque depois de instalar o Service Pack 4 ou superior, o TEM dá um erro e não deixa instalar;*
- Instalação dos Upgrades para o NNM;
- Instalação dos Upgrades para o TEM;
- Instalação dos Services Packs para NT Terminal Server;
- Upgrade para o Windows 2000 Server;
- Criação do ODBC para interligação à DataWareHouse em SQL Server;

O Observer Suite funciona de modo independente e sem integração possível com o NNM nesta versão, pelo que foi instalado posteriormente, não havendo nenhuma nota a registar sobre o processo de instalação.

4.6.2 Configuração do NNM

Anteriormente, foram definidos vários requisitos aos quais o NNM devia dar resposta, sendo para isso necessário proceder a todo um trabalho de configuração que permita uma resposta da aplicação com os contornos pretendidos, trabalho que será descrito com algum pormenor no texto que se segue.

Antes de proceder à configuração do NNM foi necessário configurar alguns equipamentos de rede (encaminhadores, comutadores, concentradores, servidores e outros sistemas clientes), para suportarem e disponibilizarem o acesso através de SNMP, direccionando toda a informação para a estação de gestão.

A configuração, quer do NNM, quer do equipamento de rede, foi efectuada em simultâneo e faseada no tempo, tendo sido primeiramente configurados os parâmetros SNMP dos equipamentos do CIC, em conjunto com os variáveis relativas a esses equipamentos na estação de gestão, e seguidamente as restantes equipamentos da UA sob a responsabilidade do CIC.

4.6.2.1 Mapas

O NNM efectua a descoberta automática da rede, organizando-a e apresentando-a ao utilizador segundo um algoritmo pré-definido. Numa rede com alguma complexidade é necessário proceder, tanto à restrição do número de objectos num determinado mapa, como à sua organização, de modo a tornar o mapa legível.

A Figura 4.52 e a Figura 4.53 apresentam dois exemplos de mapas que evidenciam o que foi referido. A primeira apresenta um mapa construído pelo NNM e a segunda, um mapa organizado de acordo com a distribuição real dos equipamentos.

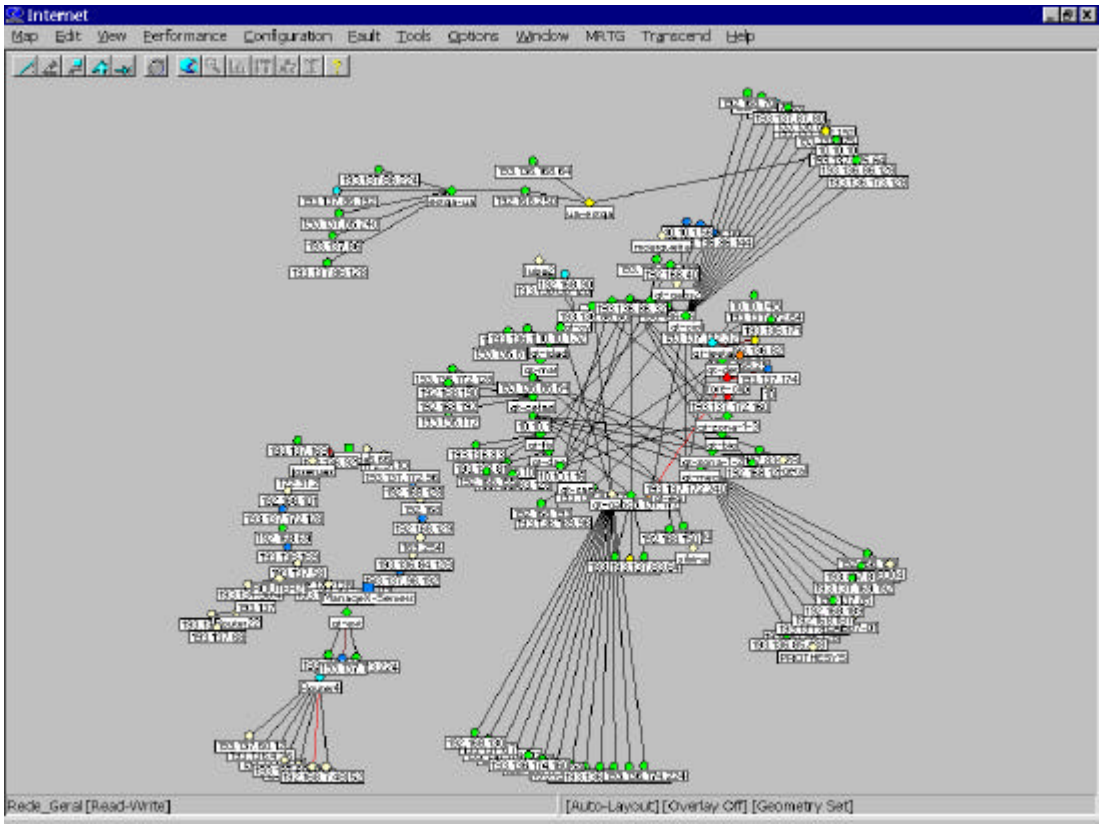


Figura 4.52 – Rede organizada pelo NNM.

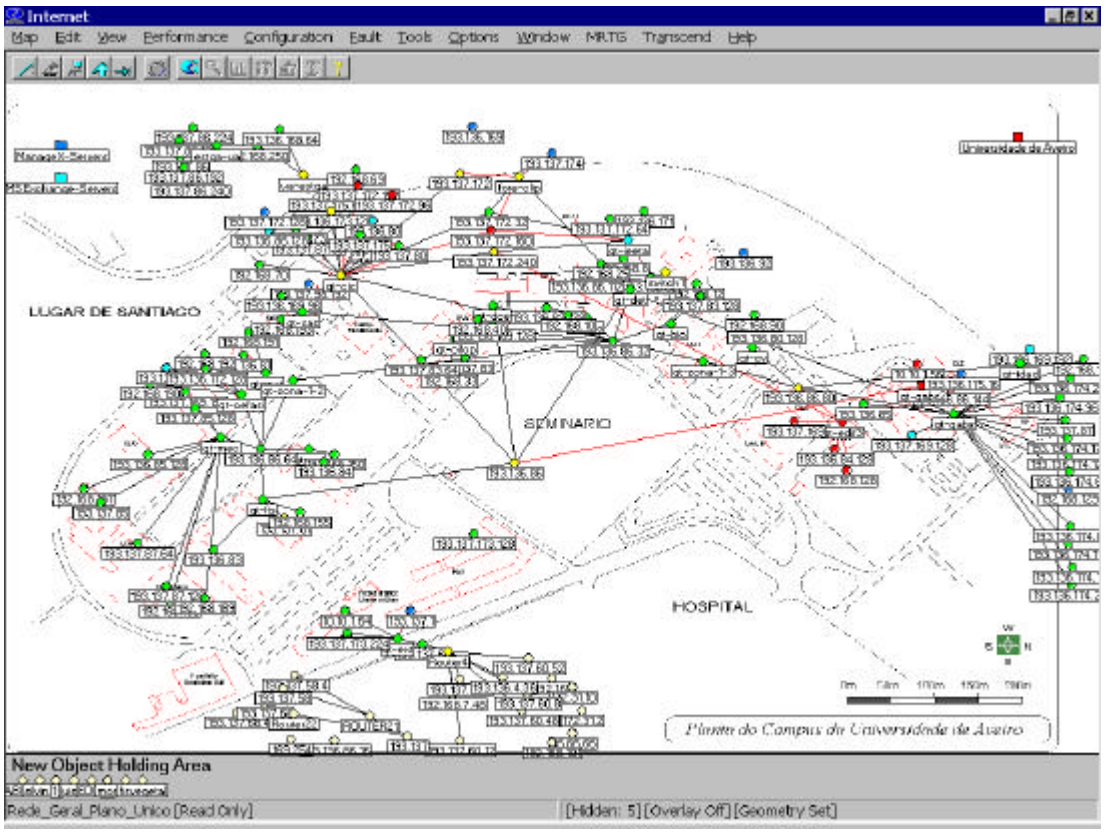


Figura 4.53 – Rede com os objectos dispostos manualmente.

Quando o NNM inicia a descoberta da rede todos os objectos são colocados num mesmo mapa com o nome *default*. A partir daqui, os vários mapas com informação diferente, serão construídos filtrando a informação que é visualizada, através da definição de filtros que irão limitar os objectos visualizados, tanto no tipo como na quantidade, através da definição de fatias de endereços e características dos equipamentos. A definição dos filtros é feita editando directamente o ficheiro de configuração (\openview\conf\filters) através de instruções booleanas, sendo apresentados na Figura 4.54 exemplos dos filtros que limitam os objectos do mapa, aos equipamentos da rede geral e às redes associadas.

```
1. {Rede_Local_EGI IPAddress ~ 193.136.84.1-126}
2. {Rede_Local_MAT IPAddress ~ 193.136.81.* & 192.168.191.* }
3. {Equi_Rede_Geral IPAddress ~ 193.136.86.* and ISRouter}
```

Figura 4.54 – Exemplos de filtros.

Posteriormente à descoberta inicial, onde o NNM colecciona os objectos e os dispõe no mapa *default*, poderá ser efectuada uma organização manual dos objectos, permitindo o rearranjo dos objectos de acordo com a estrutura física ou lógica da rede. Estes arranjos podem ser auxiliados pela atribuição de imagens de fundo aos mapas (Figura 4.55) do tipo GIF ou JPEG e representando qualquer espaço físico ou modelo organizacional: um país, uma região, um *campus*, um edifício, uma sala, a administração, o departamento de vendas, etc. A reorganização dos objectos, a atribuição de telas de fundo e a organização hierárquica do NNM, associados à funcionalidade de zoom do NNM, permitem a representação exacta das localizações físicas dos equipamentos por sub-mapa, indo até ao pormenor do canto da sala onde o computador está ligado. Na Figura 4.55 é apresentada o mapa da rede do CIC, de acordo com a localização física dos equipamentos, com uma organização que passa a assumir um carácter permanente.

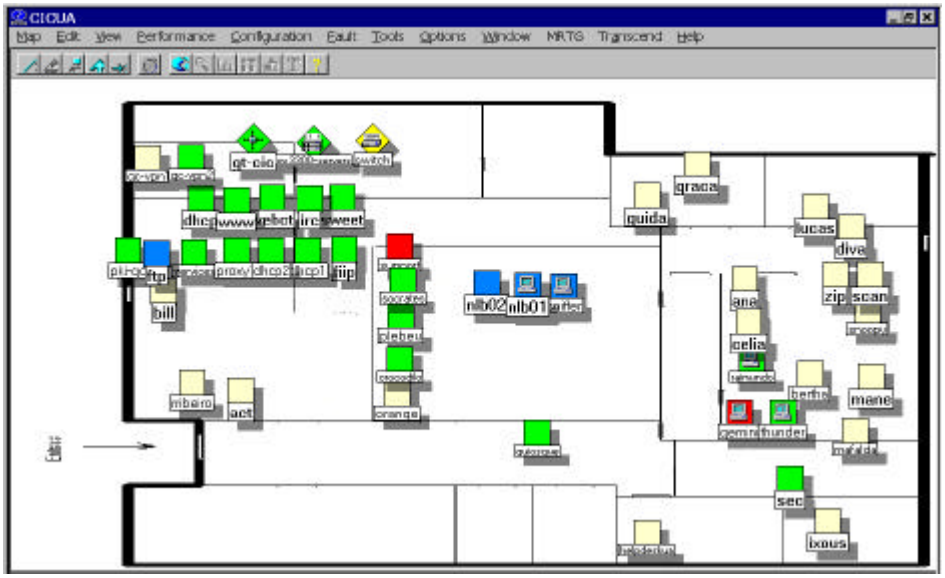


Figura 4.55 – Mapa do CIC com a respectiva planta e localização dos equipamentos.

4.6.2.2 Parâmetros SNMP

Numa rede de grandes dimensões, os equipamentos de rede podem ter parâmetros de configuração SNMP diferentes, nomeadamente no que diz respeito à *community string*. Eventualmente existirão equipas com funções distintas a realizar tarefas de gestão e que naturalmente possuirão um acesso limitado ao seu domínio de acção, havendo um centro operacional cujos membros têm acesso a todos os equipamentos.

No centro de operação da rede e a partir da estação gestora, deverá ser assegurado o acesso a todos os equipamentos de forma a executar as tarefas de manutenção e gestão necessárias, sendo para isso necessário o conhecimento de todas as *community strings* da infra-estrutura. Prevendo a situação de haver vários gestores, com alguma independência de acção, o NNM disponibiliza uma interface para a especificação deste parâmetro com uma granularidade que vai desde um domínio ou rede IP até um equipamento singular (Figura 4.56).

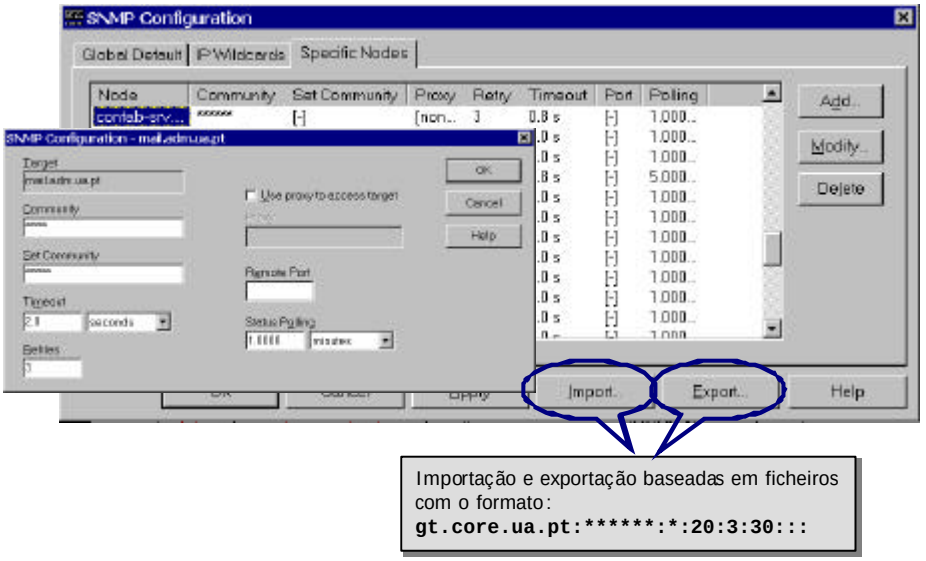


Figura 4.56 – Configuração do polling dos objectos.

A interface gráfica é útil para fazer a manutenção, mas não é versátil o suficiente para fazer uma configuração inicial de vários equipamentos de uma vez só, situação onde é útil o mecanismo de importação e exportação disponibilizado, que possibilita que os vários parâmetros sejam configurados, por exemplo, numa folha Excel e depois importados para dentro do sistema de *polling*.

4.6.2.3 Polling

As operações de gestão geram, impreterivelmente, tráfego na rede, sendo necessário tomar precauções de forma a limitar o tráfego de gestão na rede de modo a que ele próprio não constitua um elemento de congestionamento. Existem alguns processos cujo controle é complicado, como é o caso da descoberta inicial da rede, mas existem outros, como é o

caso da verificação do estado dos objectos que podem ser controlados pelo gestor. Com o intuito de controlar o tráfego, é aconselhável que todos os objectos sem importância essencial para o funcionamento da rede (como é o caso dos PCs clientes) sejam colocados no estado "não geridos", esta opção fará com que o NNM não verifique o seu estado, evitando sobrecarregar a rede com tráfego desnecessário e permitindo que objectos de importância mais relevante possam ser verificados com maior frequência.

Os três tipos de equipamentos, identificados à partida como essenciais para o funcionamento da infra-estrutura, foram os encaminhadores, equipamentos de rede local (concentradores e comutadores) e servidores de rede locais, sendo configurados, para cada um destes equipamentos, os valores de polling de acordo com as suas funções e que se indicam de seguida.

- **Encaminhadores:** 30s;
- **Servidores:** 60s;
- **Equipamentos de rede diversos:** 60s;

Para efectuar esta configuração o NNM disponibiliza uma interface gráfica que permite a configuração máquina a máquina, sendo, mais uma vez, para a configuração inicial ou alteração de todos os equipamentos, preferível utilizar ficheiros de configuração que podem ser editados externamente.

4.6.2.4 Eventos

O NNM funciona com base num sistema de eventos internos, dos quais, uma parte é disponibilizada para o gestor, fornecendo informação sobre alterações de estado, configuração e características dos objectos. Este sistema é configurável, podendo ser criados e eliminados eventos ajustando-os às necessidades de cada situação (Figura 4.57).

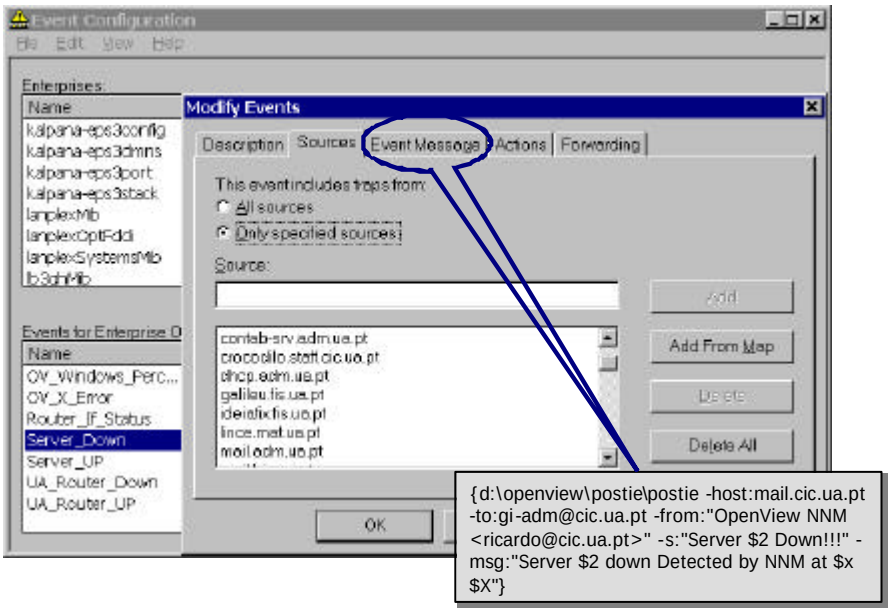


Figura 4.57 – Configuração dos alertas e mensagens associadas.

A alteração dos eventos pode ser efectuada através da interface disponibilizada pelo NNM ou através da edição directa do ficheiro de configuração, \openview\conf\trapd.conf (Figura 4.58), sendo conveniente referir que a alteração manual do ficheiro, para além de requerer grande atenção, só se justifica quando as alterações a efectuar aos eventos, nomeadamente, ao nível dos nós a monitorar e das mensagens a serem enviadas, forem de grande monta e possam ser automatizadas, por exemplo através de uma script. Caso contrário é preferível a alteração através da interface gráfica, que para além de ser bastante intuitiva não proporciona a ocorrência de erros que afectem o funcionamento do sistema.

```
EVENT Cisco_reload .1.3.6.1.4.1.9.0.0 "Cisco Alarms" Warning
FORMAT Cisco_reload trap received from enterprise $E with $# arguments:
sysUpTime=$1; whyReload=$2
EXEC d:\openview\postie\postie -host:mail.cic.ua.pt -to:deus@cic.ua.pt
-from:"OpenView NNM<ricardo@cic.ua.pt>" -s:"$r RELOAD" -msg:"Received
trap \n \t on $x at  $X from $r"
SDESC
This event occurs when an Cisco entity is reinitializing.
```

Figura 4.58 – Formato dos eventos no ficheiro de configuração, trapd.conf.

No presente trabalho havia a necessidade de enviar alertas por correio electrónico para elementos do CIC responsáveis por cada área, pelo que, nesta fase foram configurados os eventos descritos abaixo, utilizando as configurações temporais e de SNMP, definidas nos pontos anteriores.

- **Server_Down** – evento que irá alertar os gestores dos Servidores de Rede baseados em NT e Novell, para o facto do servidor não se encontrar acessível;
- **Server_UP** – em oposição ao anterior, este evento notificará que o servidor em questão já se encontra acessível;
- **Router_If_Down** – Dado que os encaminhadores possuem várias interfaces, é necessário monitorar cada uma em específico, de forma a identificar se alguma delas se encontra inactiva;
- **Router_If_UP** – mais uma vez, em oposição ao anterior, este evento irá notificar que a interface em questão voltou ao seu estado activo;

O envio de correio electrónico não é intrínseco ao NNM, sendo necessário recorrer a aplicações de terceiros que permitam, através de uma linha de comando, enviar uma mensagem configurada para os responsáveis pelo equipamento em questão com os elementos relativos ao evento. A aplicação escolhida é de domínio público e dá pelo nome *postie*, sendo apresentada na Figura 4.57, um exemplo de uma das acções desencadeadas pela geração de um evento e que procede ao envio de uma mensagem de correio.

4.6.2.5 Colecção de Dados Estatísticos

A infra-estrutura de comunicações sob análise, encontra-se em operação há já alguns anos, sofrendo de alguns problemas que, intuitivamente, apontam para congestionamentos em determinados pontos, mas cuja certeza carece de confirmação.

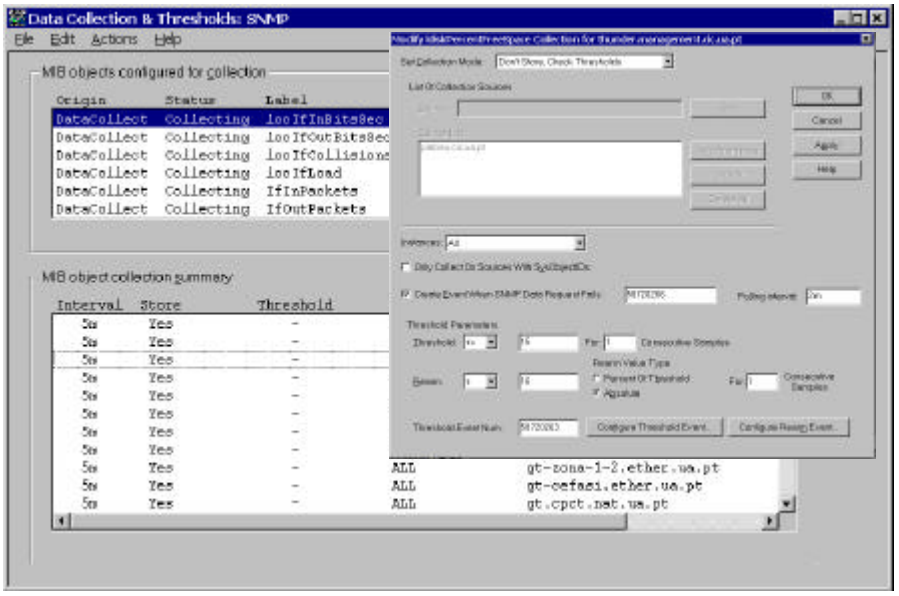


Figura 4.59 – Configuração das colecções de dados.

Numa fase inicial, e tendo em conta que se pretendiam analisar concretamente estes pontos, optou-se por implementar a colecção de dados em todos os encaminhadores do *campus*. Esta aproximação permitirá, não só, verificar os pontos de congestionamento, como também, quem são os grandes contribuidores para esta situação, possibilitando a concepção de reestruturações adequadas.

As colecções implementadas dizem respeito ao tráfego de entrada e saída, às colisões e aos erros nas interfaces, tendo sido implementadas através da interface de configuração (Figura 4.59). Convém, no entanto, referir que as colecções podem ser implementadas para qualquer outra variável disponibilizada por qualquer agente SNMP.

4.6.2.6 Data Warehouse

O armazenamento dos dados recolhidos pela estação gestora, para posterior análise, irá permitir um melhor trabalho de planificação e estruturação da rede e facilitar o acesso à informação por vários meios. Tendo em vista os objectivos enumerados, foi criada uma base de dados num servidor Microsoft SQL, a qual é acedida através de um driver ODBC implementado na estação gestora e que irá constituir o armazém de dados do NNM (Figura 4.60).

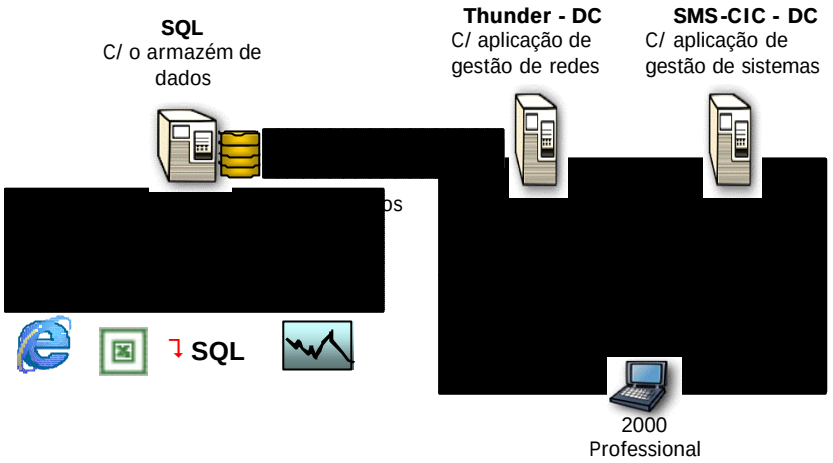


Figura 4.60 – Configuração do armazém de dados.

Os parâmetros do driver ODBC têm algumas particularidades, cuja menção é importante, para que as ferramentas de exportação funcionem correctamente, pelo que as opções seleccionadas devem ser as indicadas na Figura 4.61

Depois de criado o ODBC, a criação do armazém de dados é feito pelo NNM, através do comando: *"ovdwconfig.ovpl –rdb OVSQL -load –type msSqlSrvr"*

Este comando cria várias tabelas, que podem ser divididas em três grupos distintos:

- **Topologia**: este conjunto é constituído por 9 tabelas que contém toda a informação sobre características, topologia, ligações e interfaces dos objectos que representam os equipamentos da infra-estrutura.;
- **Eventos**: ao grupo dos eventos correspondem 10 tabelas com informação, sobre todos os eventos gerados pelo NNM, os objectos que estiveram na sua origem, a data e outras variáveis associadas;
- **Estatísticas**: as 8 tabelas deste grupo, armazenam as estatísticas recolhidas pelas colecções do NNM, sobre os objectos nelas configurados.

Depois de criadas as tabelas que constituem o armazém de dados, a sua actualização poderá ser efectuada por um de dois modos, automático ou manual. De raiz, o NNM efectua a exportação dos dados estatísticos duas vezes por dia (00H40 e 12H40), sendo a exportação dos restantes dados escalonada pelo gestor, permitindo a salvaguarda de toda a informação de acordo com a taxa de alteração da informação nas bases de dados do NNM.

A informação que requererá mais cuidado será a relativa aos eventos, uma vez que a base de dados tem um tamanho fixo, sendo rescritos os eventos mais antigos. Assim os comandos necessários à exportação dos dados para as tabelas no servidor SQL são:

"ovdwtopo –export –rdb OVSQL –v"

"ovdwevent –export –rdb OVSQL –v"

"ovdwtrend –export –rdb OVSQL –v"

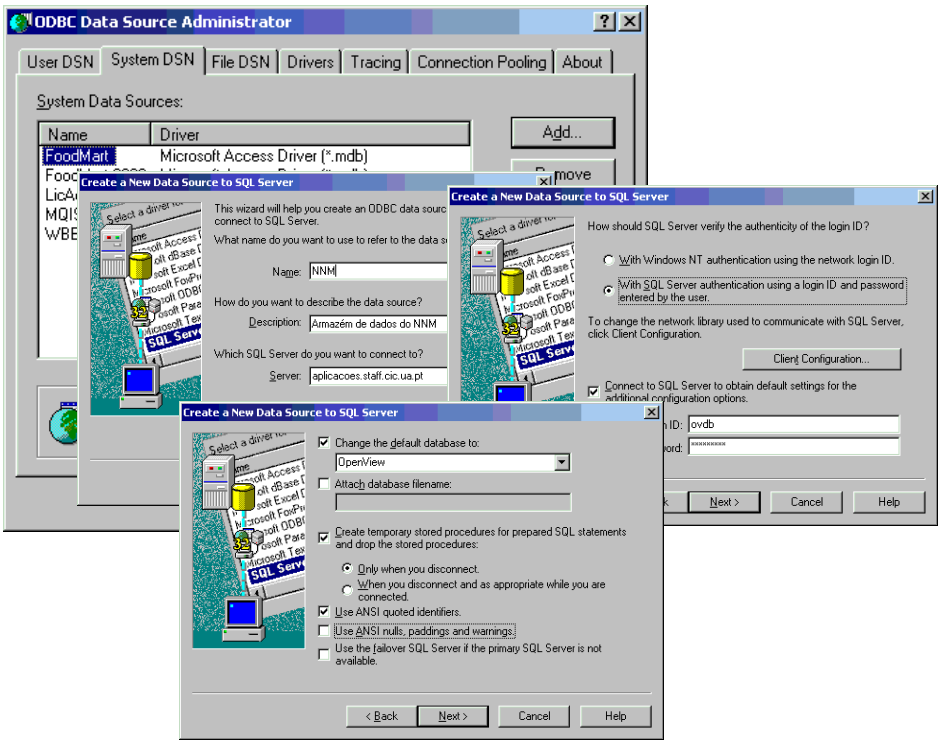


Figura 4.61 – Configuração do connector ODBC.

A consulta ao armazém de dados será apenas efectuada na medida das necessidades, ficando o desenvolvimento de uma interface generalista de acesso à informação para um trabalho futuro.

4.6.2.7 Políticas de Backup

Levando em conta que, depois da fase inicial em que as alterações à configuração e à própria base de dados são constantes, as modificações serão pequenas, a política de cópias de segurança será implementada, em primeiro lugar, utilizando o "ovbackup.ovpl" para criar uma imagem da informação e seguidamente será utilizado o *Backup Exec* para efectuar uma cópia periódica para um dispositivo de fita magnética.

4.6.2.8 Interface WEB

A dimensão do *campus* e a dispersão de equipamentos cria a necessidade de aceder à estação de gestão, fora das instalações do CIC. Atendendo aos recursos existentes nos vários edifícios da UA e aos mecanismos de acesso disponibilizados pela estação gestora, os browsers de WWW são os mais fáceis de encontrar, pelo que se optou pela implementação da interface WEB.

A configuração da interface Web visou disponibilizar, por este meio, o maior número possível de funcionalidades, pelo que foi alterado o ficheiro de registo *jovw.wrlf*, para aceder a vários mapas, eventos e informação estatística.

4.6.3 Configuração do TEM

A Central de Gestão do TEM organiza os vários equipamentos 3COM, disponibilizando o acesso a uma série de ferramentas e operações a serem executadas sobre eles.

Uma vez que a base de dados do TEM não se integra com a do NNM, são disponibilizados mecanismos de importação que permitem a adição automática dos objectos 3COM, a partir do mapa do NNM. Neste caso, a Central de Gestão do TEM deverá ser lançada, a partir do menu do NNM e, posteriormente, deverão ser importados os objectos da 3COM. Este procedimento poderá ser efectuado sempre que haja necessidade de sincronizar a base de dados do TEM e do NNM, no que diz respeito aos equipamentos da 3COM (Figura 4.62).

Uma vez que todos os equipamentos utilizados estavam sob a gestão do CIC, não foi necessário proceder a alterações nos parâmetros base de acesso aos mesmos.

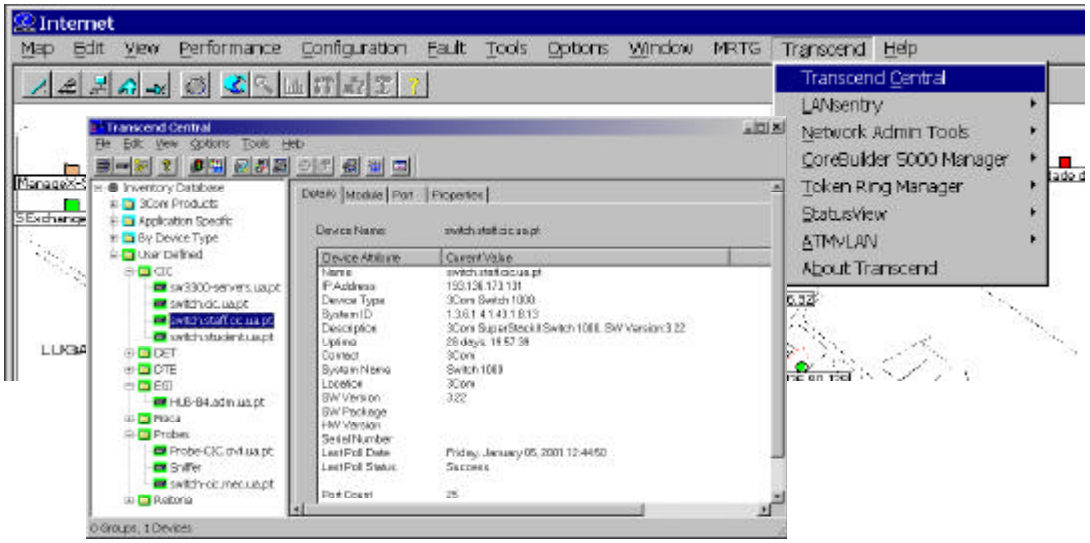


Figura 4.62 – A consola do TEM com os equipamentos agrupados.

Depois da fase inicial, esta aplicação não requer nenhuma configuração especial sendo apenas necessário agrupar os equipamentos da forma mais conveniente, por exemplo criando vários grupos correspondentes à localização física dos equipamentos. É também de referir que, caso seja conveniente, se pode proceder à inclusão e alteração manual dos equipamentos na base de dados.

No que diz respeito à configuração dos equipamentos, apenas foram predefinidos os parâmetros relativos à configuração IP e SNMP dos mesmos, não tendo sido aproveitadas, por enquanto, outras potencialidades como a criação de VLANs.

O TEM possui uma interface dedicada à actualização do software dos equipamentos. No entanto, a actualização das versões do software é complicada e só pode ser efectuada manualmente, optando-se, porque o processo é bem mais simples, por efectuar a actualização do software dos equipamentos através de um servidor TFTP (o TFTP da 3COM)

À semelhança do que acontece com o NNM, a interface WEB disponibilizada pelo TEM possibilita o acesso e configuração de todos os equipamentos da 3COM, a partir de um ponto central. Esta facilidade, por várias razões que já foram enumeradas ao longo deste trabalho, é de extrema importância facultando o acesso às ferramentas, a partir de um qualquer browser Web e a sua configuração não requer nenhum cuidado especial, bastando seguir os passos indicados pelo processo de instalação.

4.6.4 Configuração do Observer

A monitorização remota dos troços de rede requer a existência de uma sonda que possa ser deslocada de local para local. Assim o Distributed Observer foi configurado utilizando dois computadores, num deles, na estação de gestão de redes, foi instalado o Observer, no outro foram instaladas a sonda RMON e sonda Advanced Observer, disponibilizadas pelo Observer.

A primeira função atribuída a este sistema foi a monitorização e caracterização do tráfego para o exterior, cujos resultados serão apresentados no próximo capítulo.

4.6.5 Configuração dos Equipamentos

Como os diversos equipamentos da infra-estrutura da Universidade de Aveiro possuem facilidades de gestão, é necessário proceder à configuração dos vários parâmetros, criando as condições necessárias ao estabelecimento da comunicação entre os equipamentos e a estação gestora, tirando partido das facilidades implementadas.

Nesta perspectiva, em primeiro lugar, foi activado o SNMP e foram estabelecidos e configurados os parâmetros essenciais, designadamente, a *community string*, a autenticação e destino dos *traps*, e a informação sobre a localização, contacto e nome do equipamento.

Nos equipamentos Cisco, a configuração do SNMP pode ser feita utilizando o CiscoWorks ou através de linha de comandos (Figura 4.63), tendo sido este o método utilizado, através da introdução dos comandos abaixo.

```
✍✍ snmp-server community ***** RO
✍✍ snmp-server trap-authentication
✍✍ snmp-server contact BJ /RTM / CICUA - 22299
✍✍ snmp-server enable traps config
✍✍ snmp-server enable traps snmp
✍✍ snmp-server host 193.136.173.170 *****
✍✍ gt-01#_
```

Figura 4.63 – Activação e configuração do agente SNMP num encaminhador Cisco.

Os equipamentos 3COM têm uma interface de configuração ligeiramente diferente, baseada num esquema de menus de texto e que são apresentados na Figura 4.64.

```
Select menu option (snmp):

Menu options: -----------3Com SuperStack II Switch 3300-----------
 community          - Set the SNMP community strings
 get                - Get SNMP objects
 next               - Getnext SNMP objects
 set                - Set SNMP objects
 trap               - Administer SNMP trap destinations

Type "q" to return to the previous menu or ? for help.
---------------------------Switch3300 - Servers (1)--------------
Select menu option (snmp):_
```

Figura 4.64 - Activação e configuração do agente SNMP num comutador 3COM.

4.7 Configuração da Plataforma de Gestão de Sistemas

Neste ponto vai merecer a atenção, a instalação e configuração da plataforma de gestão de sistemas, cuja constituição visará dotar o CIC de mecanismos de gestão de sistemas clientes e servidores, num parque informático que conta com cerca de 2500 computadores, e cuja manutenção deverá requer o máximo de tecnologia e o mínimo de recursos humanos.

Como já foi referido não existe uma integração directa entre as duas plataformas, daí a opção por referenciar as duas áreas de forma independente, se bem que a gestão e a análise dos problemas tenha de ser feita de uma forma global e integrada, tarefas que caberão ao gestor.

4.7.1 Instalação

No seguimento dos procedimentos efectuados para a plataforma de gestão de redes foi adicionada ao domínio NT, uma nova máquina, onde foi instalado o SMS, apresentando a plataforma global a configuração representada na Figura 4.65

Depois de executados os trabalhos de instalação, a ordem dos passos necessários convém ser referida, sendo apresentada nos pontos seguintes.

- Instalação do SO Windows 2000 Server com os seguintes componentes:
  - *Internet Information Server ;*
  - *Terminal Services;*
  - *SNMP;*
- Instalação do SMS
  - *SMS;*
  - *Cristal Reports;*
  - *Network Monitor;*
  - *Ligação ao servidor MS SQL versão 7;*
- Instalação dos Services Packs do SMS
- Instalação dos Services Packs do Windows 2000

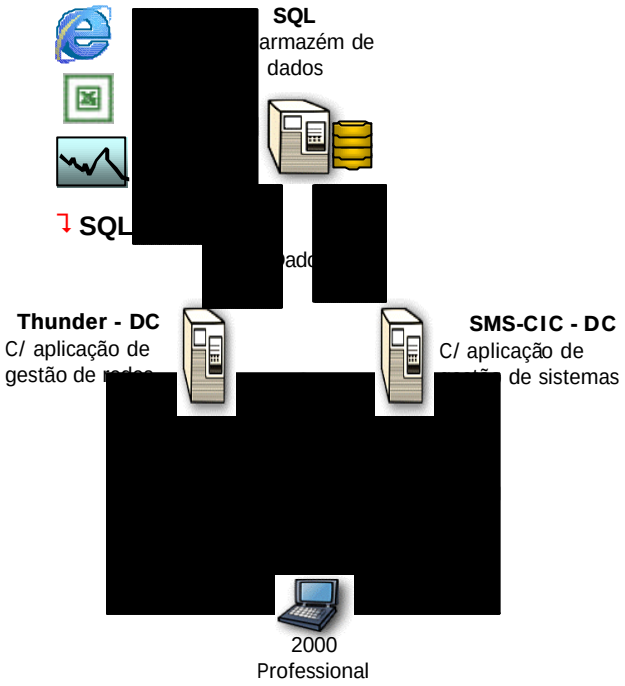


Figura 4.65 – Configuração global da plataforma.

4.7.2 Configuração do SMS

Depois de instalado, toda a configuração do SMS é efectuada através da consola *Microsoft Management Console* (MMC), tendo-se procedido às configurações iniciais com vista à descoberta da infra-estrutura. Numa primeira fase optou-se por estender todas as funcionalidades da plataforma apenas aos equipamentos do CIC, enquanto que os restantes equipamentos serão apenas identificados e colocados na base de dados. O inventário será efectuado em todos os clientes, tendo para isso sido activados os agentes de inventário quer de hardware, quer de software.

4.7.2.1 Configuração dos Domínios NT

A instalação do software relativo aos diversos papéis desempenhados pelos sistemas no contexto do SMS, é feita de forma automática bastando para isso que, na consola de administração, seja atribuído o respectivo papel ao sistema em questão, encarregando-se o SMS de proceder à instalação, desde que tenham sido estabelecidas as permissões correctas.

Para efectuar a autenticação do SMS, optou-se por implementar uma política de relações de confiança entre domínios numa configuração *single master*, sendo o domínio MANAGEMENT o master de todos os outros (Figura 4.66) iniciando-se pelo CIC que será o primeiro a ser integrado na aplicação.

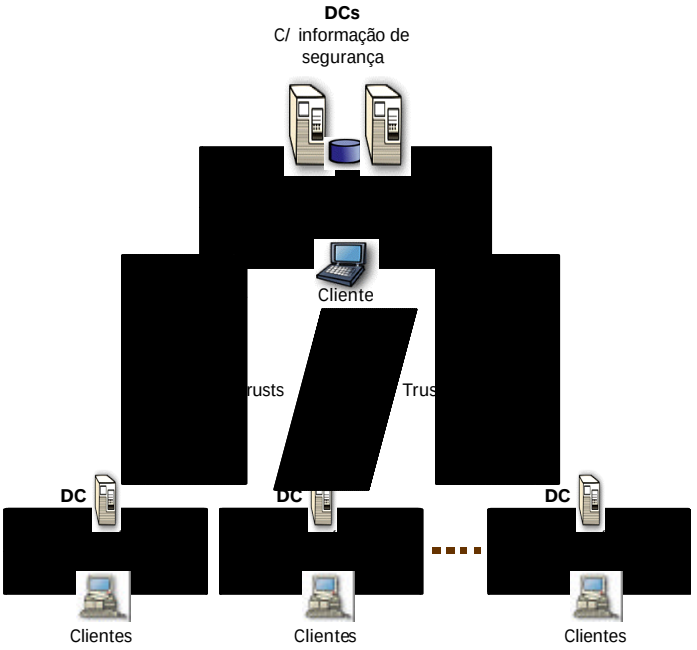


Figura 4.66 – Relações entre domínios NT.

4.7.2.2 Descoberta da Rede

No processo de descoberta da rede, e utilizando apenas um servidor de sítio e um armazém de dados, os limites de acção do sítio SMS foram definidos como sendo todas as redes IP da Universidade de Aveiro. A descoberta dos clientes foi configurada para usar qualquer dos processos disponíveis (Figura 4.67), afim de se popular rapidamente o armazém de dados, incluindo informação sobre os sistemas e topologia de rede onde estão inseridos.

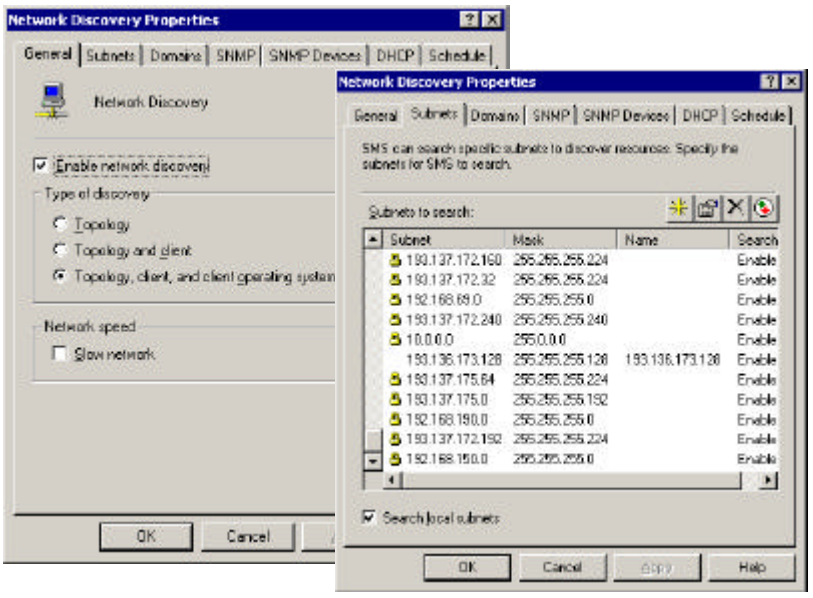


Figura 4.67 – Interface de configuração da descoberta da rede.

4.7.2.3 Instalação dos Clientes

A instalação dos clientes pretende-se controlada pelo que apenas três domínios e sub-redes foram configuradas como pertencentes à fronteira de gestão do servidor SMS, tendo sido escolhida, de entre os vários processos de instalação do software cliente, a instalação através de *logon scripts*. Assim, foram designados os três domínios, como ponto de instalação e, automaticamente, aos seus controladores de domínios foi-lhes atribuído o papel de *logon points*, tendo sido modificadas as scripts de logon para procederem à instalação dos agentes nos computadores pessoais.

A execução deste ponto foi efectuada tendo em conta o modelo de segurança e relações de confiança, definido para os domínios da UA. Eventuais problemas com a instalação devem ser analisados os logs, armazenados, quer no servidor SMS, quer nos clientes e pontos de distribuição.

4.7.2.4 Distribuição de Software

Numa primeira fase, servindo apenas de experimentação, foi configurada a distribuição do pacote antivírus para os computadores do CIC, sem que tenham sido impostas políticas de instalação pelo gestor. Não tendo sido feita nenhuma modificação ao pacote de instalação do antivírus, os clientes apenas serão advertidos de que existe o pacote para instalação e poderão optar por instalar, ou não, o pacote.

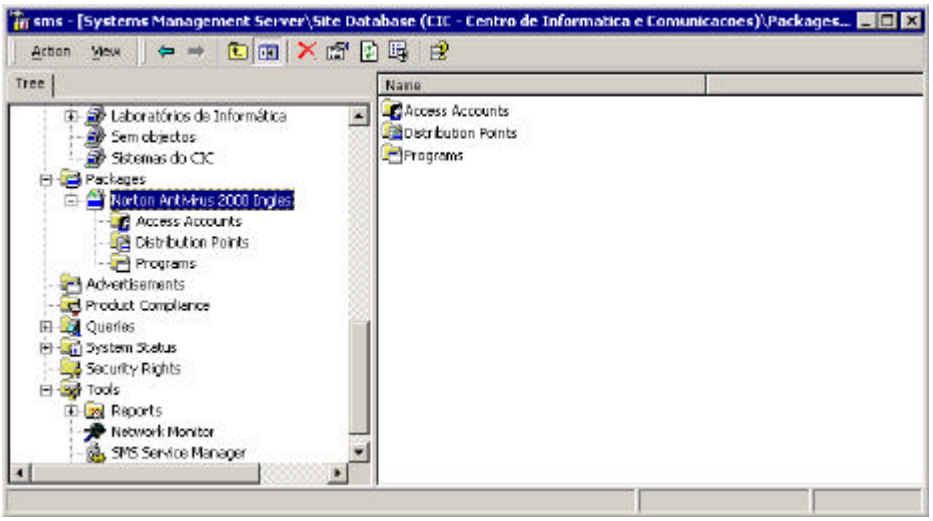


Figura 4.68 – Consola de instalação de software.

O processo de experimentação de distribuição de software foi complementado com a utilização das aplicações WinInstall LE e SMS Installer, tendo sido criados pacotes de instalação personalizados com base em diferentes métodos. Para o WinInstall usou-se a monitorização da instalação da aplicação, com base na diferença de imagens do sistema entre o pré e o pós instalação. Para o SMS Installer foi criado o mesmo pacote, mas desta

vez, baseado na monitorização dos ficheiros e chaves de registo utilizadas pela aplicação durante a sua execução.

4.8 Considerações Finais

Os trabalhos de instalação e configuração efectuados, antes de mais, permitiram uma familiarização com as aplicações e os problemas práticos da sua implementação, testando as capacidades anunciadas pelos fabricantes. Esta fase do trabalho será a base para a experimentação da solução global em todas as suas vertentes, assunto que será abordado no próximo capítulo.

5 Resultados Operacionais

5.1 Introdução

O estudo produzido relativo às tecnologias e ferramentas de gestão potenciaram a implementação de um Centro de Operações dotado de um conjunto de ferramentas que permitem efectuar uma gestão avançada de uma infra-estrutura de informática com características semelhantes à da Universidade de Aveiro. As funcionalidades disponíveis, bem como, alguns resultados obtidos na sequência da implementação do Centro de Operações, serão abordados e descritos neste capítulo.

5.2 COP – Centro de Operações

Com o objectivo de distribuir a informação de gestão pelos técnicos responsáveis pelas infra-estruturas de comunicação e informática, foram constituídos e adaptados a cada equipa mapas, eventos e estatísticas correspondentes às suas áreas de intervenção. A estrutura actual da plataforma encontra-se ilustrada na Figura 5.1 e compreende um conjunto de actores relacionado com as actividades das várias equipas do CIC, sendo a informação acedida remotamente e através dos vários métodos disponibilizados.

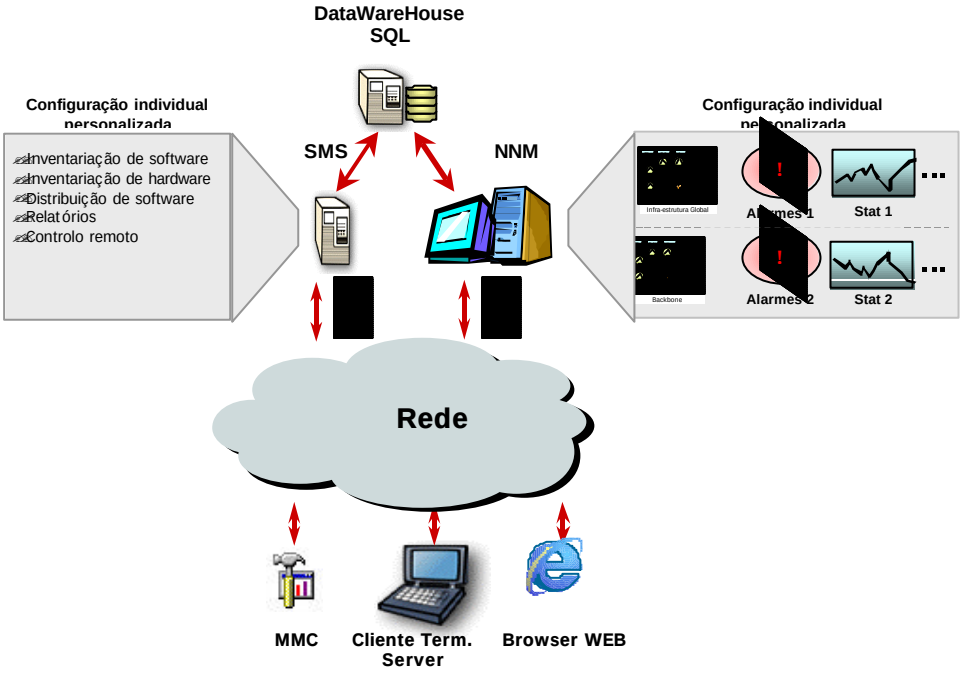


Figura 5.1 – Arquitectura do Centro de Operações implementado.

5.2.1 Mapas

Dada a dimensão da infra-estrutura informática da UA, optou-se por mostrar apenas a informação relevante para cada actividade, recorrendo-se ao uso de filtros para a criação de mapas. Foram criados três mapas distintos, o primeiro deles contém toda a infra-estrutura de informática, a partir do qual se tem uma perspectiva global do estado da infra-estrutura, designado por *"infra-estrutura_global"* (Figura 5.2).

Este mapa foi criado com o objectivo da equipe de helpdesk ter no seu monitor, a cada momento, a possibilidade de identificar algum problema que exista, em qualquer ponto da infra-estrutura.

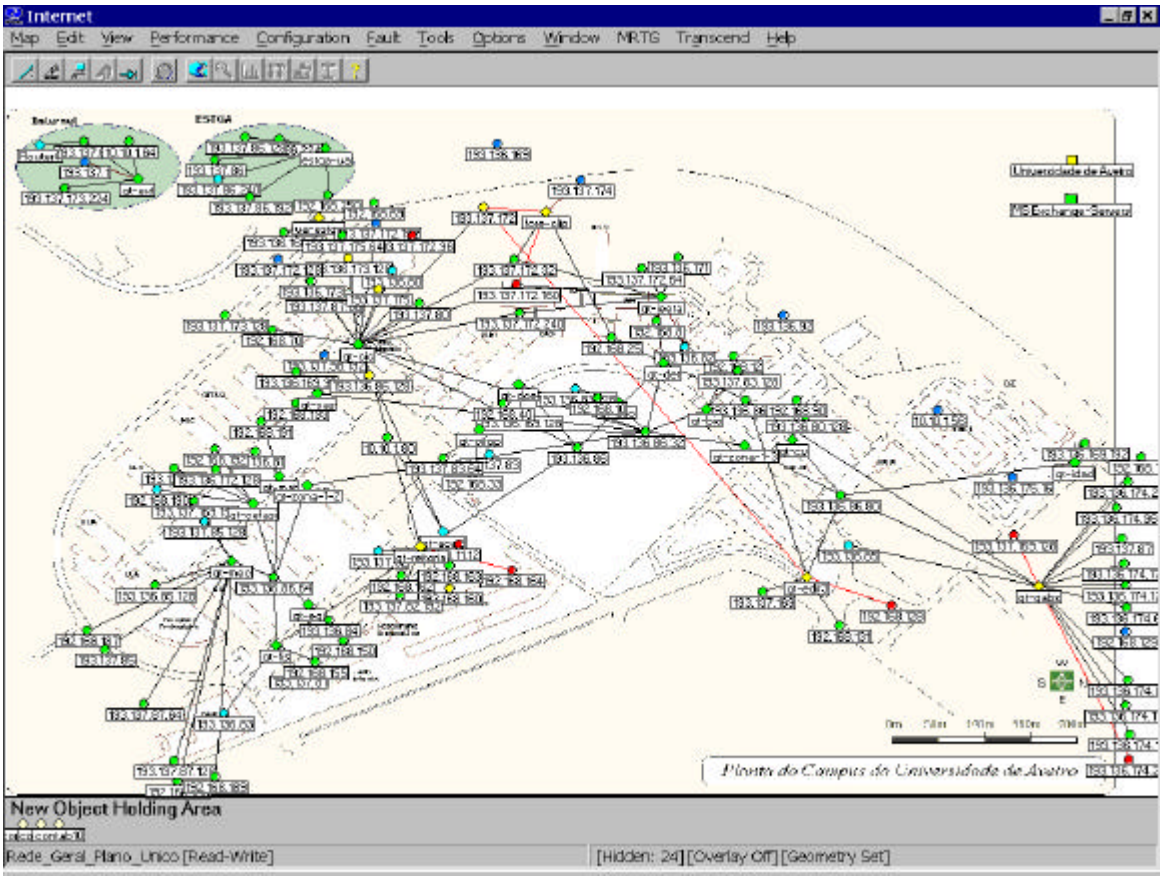


Figura 5.2 – Infra-estrutura global.

Um outro mapa criado, foi o mapa dos servidores de rede, de nome *"Servidores_de_Rede"*, destinado à equipa responsável pela gestão dos servidores departamentais, onde foram colocados os vários servidores da infra-estrutura, permitindo uma visão global de todos os equipamentos.

O terceiro mapa criado, de nome *"Backbone"* (Figura 5.3) contém apenas os objectos correspondentes aos equipamentos da rede geral, destinando-se a ser usado pela equipa responsável pela manutenção dos equipamentos da rede geral, que funciona como a espinha dorsal de toda a infra-estrutura de comunicações da Universidade.

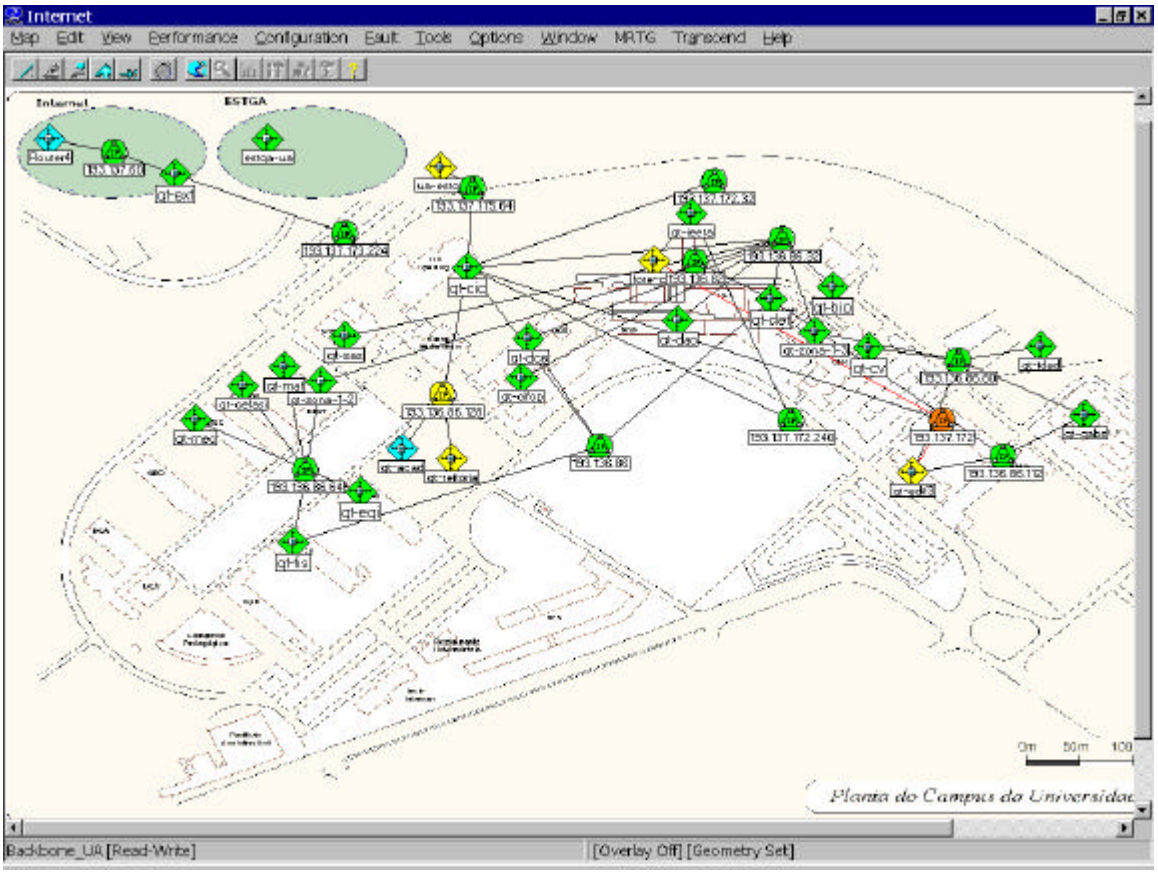


Figura 5.3 – Mapa da rede de espinha dorsal.

5.2.2 Estatísticas

No que diz respeito às estatísticas procedeu-se à implementação da recolha de estatísticas quer para equipamentos da infra-estrutura geral de comunicações, quer para equipamentos de suporte aos serviços disponibilizados na infra-estrutura da UA. Neste âmbito, foram implementadas as seguintes recolhas de estatísticas, efectuadas pelo próprio NNM e que são exportadas posteriormente para a *DataWarehouse*.

- **LocIfInBits** – bits por segundo na entrada da interface;
- **LocIfOutBits** – bits por segundo na saída da interface;
- **LocIfCollisions** – Colisões na interface;
- **LocIfLoad** – Carga da Interface;
- **ldiskPercentFreeSpace** – Ocupação do espaço em disco;

Estas estatísticas são essenciais, quer na análise das evoluções do tráfego nos vários troços de rede, quer na análise da evolução da taxa de erros ocorridos nesses mesmos troços, em função do volume de tráfego.

Relativamente aos servidores, pode ser analisada a evolução do espaço em disco, podendo prever, de antemão, a altura em que será necessário organizar o espaço, ou colocar um novo disco no servidor.

5.2.3 Eventos e Falhas

No sentido de proporcionar uma gestão activa sempre que é gerado um evento ou recebido um *trap*, indicando a alteração de condições pré-definidas ou de falha em algum equipamento, são enviadas mensagens de correio electrónico para os responsáveis pelo equipamento. O armazenamento dos eventos foi também acautelado para que cada um dos técnicos possa aceder rapidamente, apenas aos eventos relevantes para as funções que desempenha. Deste modo, foram configuradas as seguintes categorias de eventos:

- **Configuração** – Erros relativos à configuração dos parâmetros IP;
- **Routers Cisco**– Eventos e notificações relativos aos encaminhadores;
- **Servidores de rede** – Eventos e notificações relativos aos servidores de rede local;
- **3COM** – Eventos e notificações relativos aos equipamentos de comutação das redes locais;

O sistema de eventos do SMS é ligeiramente diferente, relacionando-se essencialmente com o funcionamento interno do sistema, pelo que a sua verificação é particularmente importante quando se efectuam operações sobre o sistema ou se detectam anomalias no funcionamento.

5.2.4 Inventariação de Hardware e Software

Relativamente à inventariação de hardware e software, encontram-se implementados os mecanismos necessários para que se proceda à inventariação completa da infra-estrutura de informática da Universidade de Aveiro. A inventariação do equipamento de comunicação é possível através das duas aplicações de gestão de redes (NNM e Transcend), que efectuam uma descrição bastante precisa e completa. Os computadores e software instalado são inventariados através do SMS e, desde que os clientes estejam instalados, consegue-se obter a descrição completa e pormenorizada de todo o hardware e software, incluindo os modelos dos equipamentos e as versões de software.

Ainda nesta área, os mecanismos de controlo de utilização de licenças de software podem facilmente ser implementados bastando activar a opção *Software Meetering* do SMS, que apenas foi objecto de estudo neste trabalho enquanto funcionalidade do SMS.

5.2.5 Distribuição de Software

A distribuição automática de software é uma ambição de muitos gestores de sistemas, que lhes economiza muito tempo de manutenção de sistemas. Neste trabalho foi testada e implementada a distribuição de aplicações, através do SMS, tendo sido superadas as expectativas em relação a esta funcionalidade. A distribuição foi feita criando pacotes de distribuição automática e advertindo os clientes para disponibilidade de um novo software, que o instalavam com sucesso.

5.2.6 Recolha e Análise de Tráfego

A recolha e análise de tráfego proporcionam um melhor apetrechamento na resolução de problemas e no conhecimento mais aprofundado da tipicidade dos serviços suportados e utilizados na infra-estrutura. Neste campo, o Observer desempenha um papel fundamental, disponibilizando mecanismos que permitem analisar remotamente, e de um modo distribuído, o comportamento do tráfego num troço de rede. A informação disponível através desta ferramenta é compatível com RMON2, sendo disponibilizada por um agente RMON, ou por um agente próprio que fornece mais informação que a obtida pelo agente RMON, mas que apenas pode ser utilizado pelo Observer.

5.2.7 Data WareHouse

O armazenamento da informação numa base de dados SQL permite, não só aliviar a carga da aplicação de gestão que não tem de a processar nem sustentar localmente, mas também a constituição de um repositório central de dados, possibilitando uma análise a longo prazo que permita avaliar a evolução do comportamento da infra-estrutura e fundamentar decisões relativamente a futuros aperfeiçoamentos.

5.3 O primeiro Relatório Sobre a Infra-estrutura de Comunicações

Todas as considerações sobre a instalação e configuração da plataforma partem do princípio de que a infra-estrutura está correctamente instalada e configurada. No caso da UA, dada a considerável dimensão da sua infra-estrutura e toda a sua história, esta não é uma verdade absoluta, havendo diversos problemas, quer na configuração de servidores centrais, quer na configuração individual dos clientes e equipamentos terminais. Assim, depois de implementada a plataforma, procedeu-se a uma análise inicial dos dados recolhidos com vista a elaborar um relatório preliminar de anomalias, fundamentando-o com a informação recolhida pelo NNM.

Em primeiro lugar, foram identificados erros de configuração ao nível dos valores dos parâmetros IP, através da análise dos eventos e alarmes recolhidos pelo NNM (Tabela 5.1). Os erros mais comuns foram as máscaras erradas, os endereços IP repetidos e registos errados de DNS. Nos dois primeiros casos a identificação do problema foi feita pela análise das mensagens dos alarmes gerados pelo NNM, no caso dos erros de tabelas de DNS a detecção não foi explicita e foi mesmo algo complicada, já que disposição automática dos objectos é que apresentava anomalias no funcionamento. Estas anomalias passavam pela constante alternância dos nomes dos objectos e pela junção de dois objectos num único, contendo as interfaces de ambos. Foram equacionadas várias hipóteses, incluindo o mau funcionamento do NNM até, na lista de distribuição do OpenView Fórum, ter sido encontrada uma dica com a solução para o caso: *"como o NNM usa o sistema de DNS para a identificação dos nomes, utilizando a resolução directa e inversa, se houver*

dois registos inversos do mesmo nome, para IPs diferentes, o NNM entende que os objectos são um único, com as interfaces de ambos". Os erros nos registos de DNS criavam problemas, não apenas à construção dos mapas, mas também a todo o funcionamento do NNM, sempre que se recorria a selecção de objectos para efectuar alguma operação.

Tabela 5.1 – Eventos iniciais.

Data	Origem	Evento
24-01-2000 10:00	sw3300.fis.ua.pt	sw3300.fis.ua.pt: Node marginal
24-01-2000 10:36	srv.dao.ua.pt	srv.dao.ua.pt: Inconsistent subnet mask 255.255.255.0 on interface Realtek, should be 255.255.255.128
24-01-2000 14:24	srv.egi.ua.pt	srv.egi.ua.pt: Inconsistent subnet mask 255.255.255.0 on interface OvisLink, should be 255.255.255.128
24-01-2000 16:39	srv.cifop.ua.pt	srv.cifop.ua.pt: Inconsistent subnet mask 255.255.255.0 on interface CNet, should be 255.255.255.192
24-01-2000 17:33	193.136.83.128	193.136.83.128: Network status major (almost critical)
24-01-2000 18:00	srv.dao.ua.pt	srv.dao.ua.pt: Inconsistent subnet mask 255.255.255.0 on interface Realtek, should be 255.255.255.128
24-01-2000 18:47	atm66.atm.ua.pt	atm66.atm.ua.pt: Inconsistent subnet mask 193.137.172.192 on interface el17, should be 255.255.255.224
24-01-2000 19:09	contab-srv.adm.ua.pt	contab-srv.adm.ua.pt: Node down
24-01-2000 19:09	193.137.169.Segment5	193.137.169.Segment5: Segment critical
24-01-2000 21:14	193.136.84.125	193.136.84.125: Duplicate IP address: node 193.136.84.125 reported having 192.168.101.1, but this address was previously detected on node HUB-84.adm.ua.pt
24-01-2000 23:21	srv.egi.ua.pt	srv.egi.ua.pt: Inconsistent subnet mask 255.255.255.0 on interface OvisLink, should be 255.255.255.128
24-01-2000 23:28	atm66.atm.ua.pt	atm66.atm.ua.pt: Inconsistent subnet mask 193.137.172.192 on interface el17, should be 255.255.255.224

A resolução dos problemas anteriores, nos dois primeiros casos, passa pela verificação da configuração do servidor de DHCP, na atribuição estática do endereçamento, ou pela verificação e correcção dos parâmetros IP nas máquinas clientes, onde a configuração é feita de modo manual. No caso do DNS é aconselhável rever o mecanismo de actualização de tabelas, implementando soluções que impossibilitem a introdução de erros na configuração das mesmas e, em complemento, estudar a aquisição de software de teste de configuração de DNS (Ex: *DNS Expert da Men&Mice*), que periodicamente deverá verificar a consistência e integridade das configurações dos vários domínios da UA.

5.4 Eventos e Notificações

No que respeita aos eventos e notificações, é incontestável a sua importância na gestão activa de uma infra-estrutura, realidade confirmada pelo sistema de envio de mensagens

implementado, que no intervalo de tempo máximo de um minuto, detecta e reporta a inacessibilidade dos equipamentos fundamentais para o funcionamento da infra-estrutura (Figura 5.4). Já anteriormente tinham sido implementados no CIC, mecanismos com estas funções, no entanto, a eficiência demonstrada pelo sistema de eventos do NNM é muito superior, funcionando centralmente e integrado com a plataforma global.

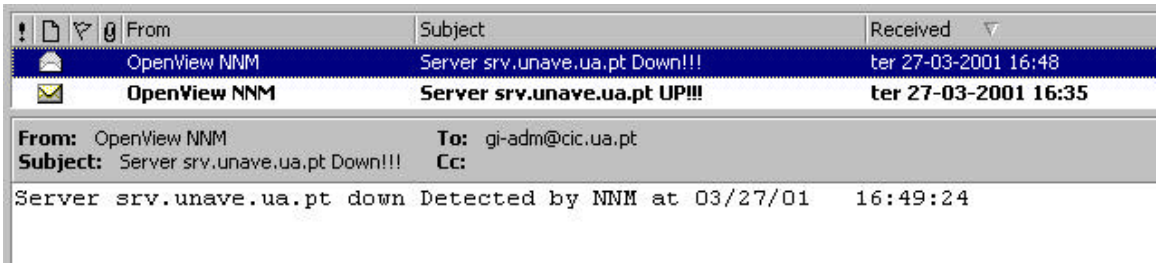


Figura 5.4 – Mensagem de correio com alerta sobre um servidor em baixo.

Como acessório a este sistema, foram identificadas as notificações recebidas dos equipamentos de comunicação e, em conjunto com os eventos internos do NNM, foi também configurada a recepção de notificações de agentes SNMP, pelo que sempre que existe uma alteração no estado de um equipamento ou interface, os responsáveis pela área são automaticamente informados da ocorrência (Figura 5.5).

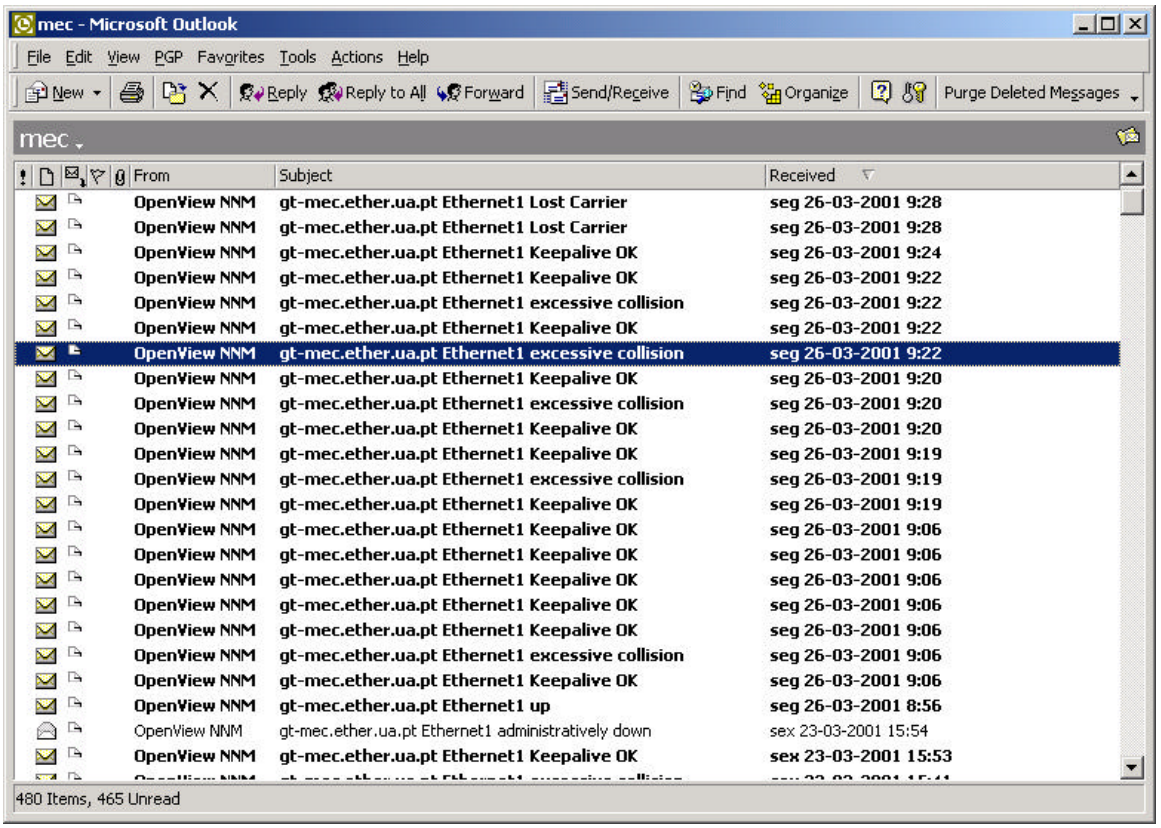


Figura 5.5 – Notificações do encaminhador GT-MEC sobre o estado da interface Etherne1.

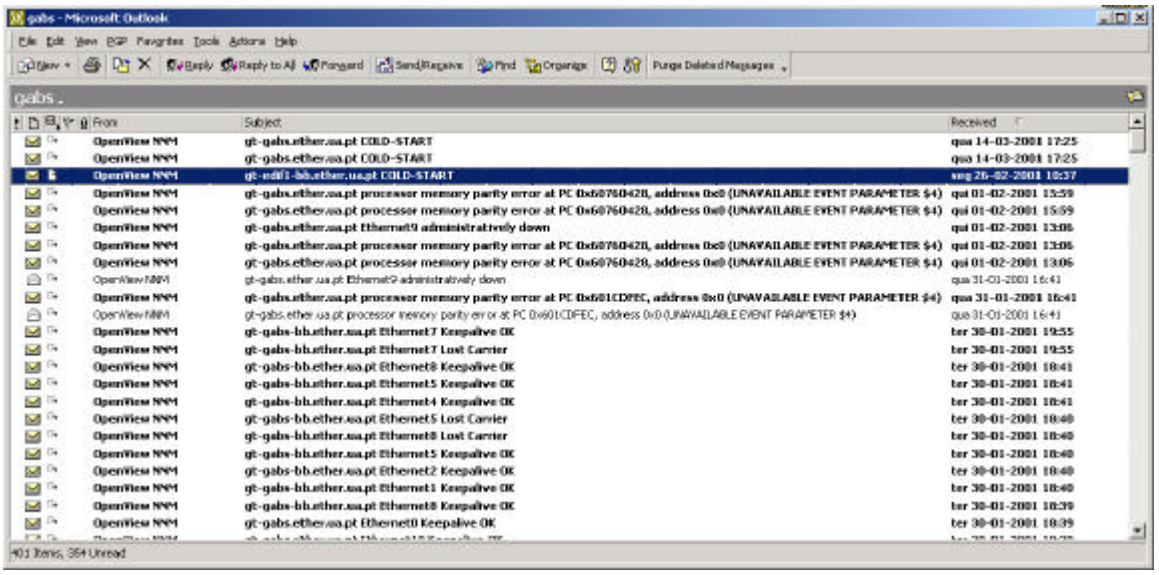


Figura 5.6 – Notificações do encaminhador GT-Gabs sobre erros de memória e alterações do estado das interfaces.

Depois de estar a funcionar o sistema de eventos do NNM, foram detectadas falhas de funcionamento em equipamentos, que até à implementação da plataforma sempre se tinham comportado "correctamente", sendo um exemplo, os erros de memória em alguns encaminhadores, que originavam a perda temporária de conectividade, mas cuja duração não era suficiente para se identificar o problema. A Figura 5.6 mostra erros de memória gerados no GT-Gabs que originavam, aleatoriamente, a perca momentânea de conectividade, que era reportada como lentidão da comunicação pelos utilizadores, mas que testes efectuados à comunicação nunca tinham revelado qualquer falha.

De um modo geral o sistema de eventos implementado, veio melhorar significativamente o tempo de resposta na identificação e resolução de problemas.

5.5 A Construção dos Mapas

Um dos requisitos era a construção e actualização automáticas dos mapas que modelam a infra-estrutura informática. Neste campo, o NNM mostra-se muito eficiente e dotado de uma série de mecanismos que mantém os mapas constantemente actualizados com o estado dos objectos. Convém, no entanto, referir que o NNM utiliza algoritmos próprios na realização destas tarefas, sendo o seu funcionamento pautado pelo seguinte procedimento: sempre que é descoberto um objecto, são executados sobre ele uma série de testes de modo a identificar as suas características e capacidades, seguidamente são verificadas as interfaces e os seus endereços, sendo atribuído ao nome dos objectos, o nome do primeiro campo, obtido por consulta à tabela DNS inversa, do endereço mais baixo de todas as interfaces. Ora, não tendo sido prevista inicialmente esta situação, a atribuição de endereços na Universidade de Aveiro, pautou-se pela disponibilidade sequencial ainda existente das redes da gama 193.X.X.X e 192.168.X.X, fazendo com que nos mapas do

NNM, os objectos não fossem identificados segundo nenhuma lógica coerente, existindo uma série de equipamentos com o mesmo nome (Ex: GT.cic.ua.pt; GT.det.ua.pt, etc.). O mesmo problema surgiu com a nomeação dos servidores, Figura 5.7.

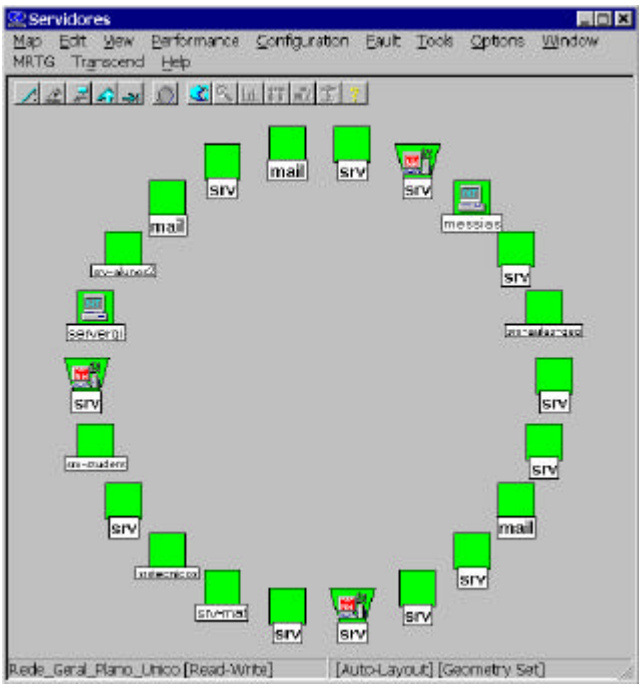


Figura 5.7 – Contentor com os servidores de rede.

Esta limitação contribuiu para a instalação da confusão na análise dos mapas, essencialmente na rede geral. Posteriormente optou-se pela configuração de uma rede privada da gama 10.X.X.X, em todos os equipamentos de comutação, passando esta a ser utilizada, quer para a identificação dos objectos, quer para a comunicação com os mesmos, com os resultados apresentados na Figura 5.8.

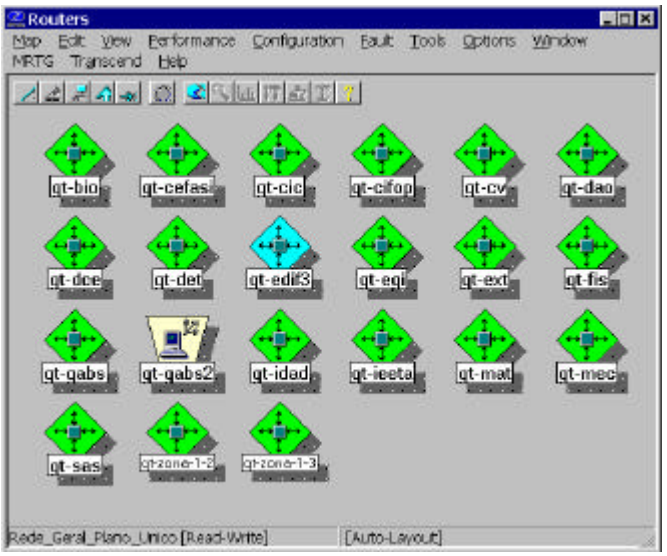


Figura 5.8 – Contentor com os encaminhadores da rede geral.

Depois da fase inicial, procedeu-se à estruturação dos mapas, que passaram a modelar a componente física da infra-estrutura (Figura 5.2) e a componente organizacional (Figura 5.9). Esta segunda ainda não está concluída, no entanto o trabalho já realizado revela a importância e as vantagens de proceder a este tipo de organização para toda a infra-estrutura. O trabalho será algo moroso, já que será necessário encontrar todas as plantas dos edifícios da UA, digitalizá-las e posteriormente, incluí-las nos mapas do NNM. O processo passará pela criação de contentores de objectos que serão hierarquizados, permitindo a navegação entre eles e facilitando a identificação, não só da origem dos problemas, mas também da localização física dessa origem, problema que se coloca sem a existência de um sistema de localização geográfica. Neste campo seria útil o estudo mais aprofundado da aplicação *IT Layers* e da sua aplicabilidade à infra-estrutura da Universidade de Aveiro.

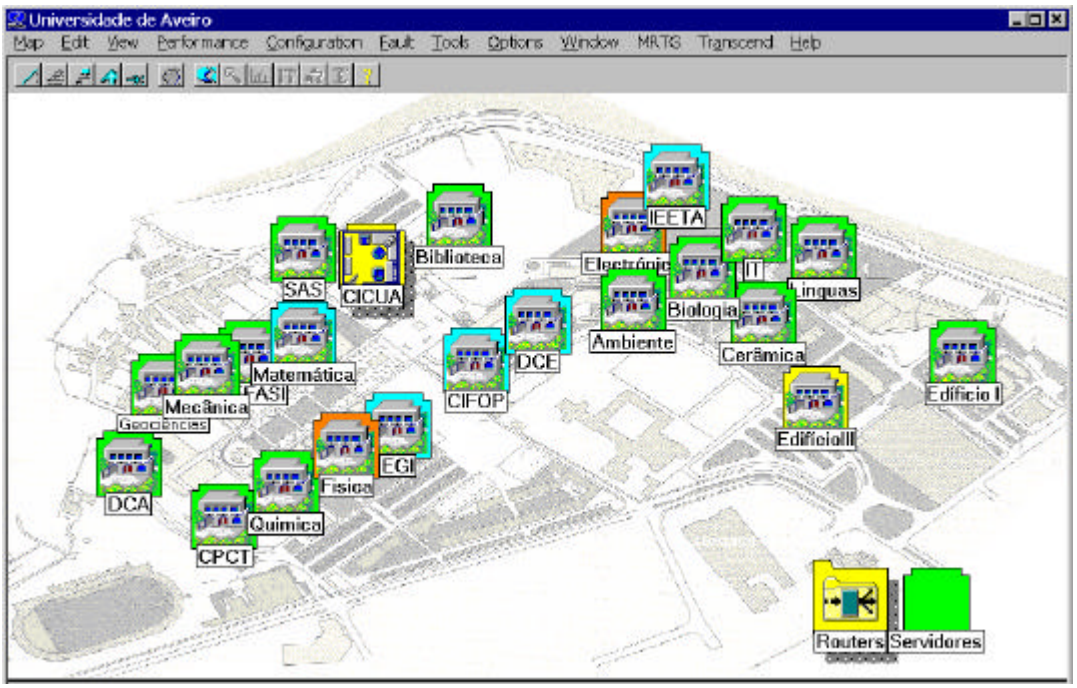


Figura 5.9 – Mapa da infra-estrutura de informática da UA organizado fisicamente.

5.6 Dados Estatísticos da Infra-estrutura da UA

A infra-estrutura Ethernet da rede geral era, desde há muito tempo, contestada pela sua sobrelotação em termos de tráfego. Existindo infra-estruturas paralelas de alto débito subaproveitadas, realizaram-se algumas medidas da quantidade de tráfego, com vista a uma reorganização da infra-estrutura, aproveitando o mais possível as tecnologias de alto débito para transportar os dados dentro do *campus* da Universidade. Na Figura 5.10, encontram-se assinalados os pontos de monitorização da rede Ethernet, tendo sido escolhidos por serem os pontos de separação entre as zonas Norte e Centro, Centro e Sul e a interligação da zona Sul com o FDDI e consequentemente com o CIC e a Internet.

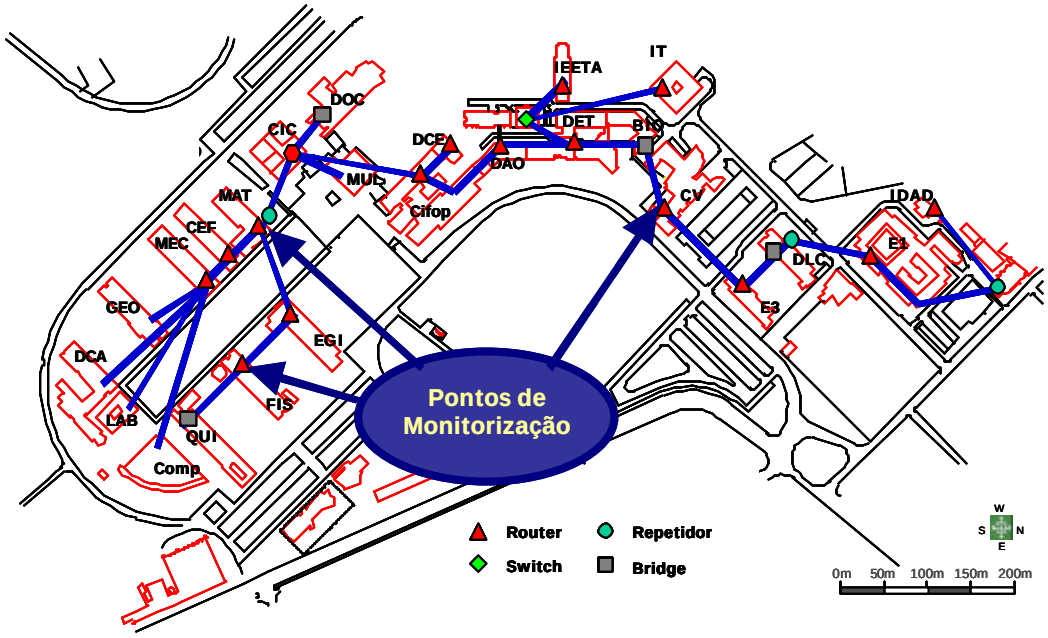


Figura 5.10 – Pontos de monitorização de tráfego na infra-estrutura geral Ethernet.

A monitorização incidiu, nesta fase, sobre o tráfego nas interfaces, a taxa de erros, a ocupação das interfaces e a carga de CPU, as medidas resultantes e relevantes encontram-se nos gráficos da Figura 5.12, Figura 5.13 e Figura 5.14. Em paralelo foram efectuados alguns testes com ferramentas vulgares como o ping (Figura 5.11).

```
Pinging gt-idad.ether.ua.pt [193.136.86.85] with 2000 bytes of data:
Reply from 193.136.86.85: bytes=2000 time=16ms TTL=253
Reply from 193.136.86.85: bytes=2000 time=16ms TTL=253
Request timed out.
Reply from 193.136.86.85: bytes=2000 time<10ms TTL=253
Reply from 193.136.86.85: bytes=2000 time<10ms TTL=253
Request timed out.
Reply from 193.136.86.85: bytes=2000 time=16ms TTL=253
Request timed out.
Request timed out.
Request timed out.
Reply from 193.136.86.85: bytes=2000 time<10ms TTL=253
Request timed out.
Reply from 193.136.86.85: bytes=2000 time<10ms TTL=253
Reply from 193.136.86.85: bytes=2000 time<10ms TTL=253
Reply from 193.136.86.85: bytes=2000 time<10ms TTL=253
Request timed out.
...
...
Ping statistics for 193.136.86.85:
    Packets: Sent = 56, Received = 37, Lost = 19 (33% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  20ms, Average =  5ms
```

```
Pinging mail.adm.ua.pt [193.136.84.252] with 2000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Reply from 193.136.84.252: bytes=2000 time=16ms TTL=125
Reply from 193.136.84.252: bytes=2000 time=16ms TTL=125
Reply from 193.136.84.252: bytes=2000 time=16ms TTL=125
Reply from 193.136.84.252: bytes=2000 time=16ms TTL=125
Request timed out.
Reply from 193.136.84.252: bytes=2000 time=16ms TTL=125
Request timed out.
Reply from 193.136.84.252: bytes=2000 time=16ms TTL=125
Reply from 193.136.84.252: bytes=2000 time=16ms TTL=125
Request timed out.
Reply from 193.136.84.252: bytes=2000 time=16ms TTL=125
Request timed out.
Request timed out.
...
...
Ping statistics for 193.136.84.252:
    Packets: Sent = 56, Received = 36, Lost = 20 (36% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum =  16ms, Average =  10ms
```

```
Pinging srv.cemed.ua.pt [193.137.87.15] with 2000 bytes of data:
Reply from 193.137.87.15: bytes=2000 time=16ms TTL=125
Request timed out.
Request timed out.
Reply from 193.137.87.15: bytes=2000 time<10ms TTL=125
Reply from 193.137.87.15: bytes=2000 time<10ms TTL=125
Reply from 193.137.87.15: bytes=2000 time=15ms TTL=125
Request timed out.
Reply from 193.137.87.15: bytes=2000 time<10ms TTL=125
Reply from 193.137.87.15: bytes=2000 time<10ms TTL=125
Reply from 193.137.87.15: bytes=2000 time=15ms TTL=125
Request timed out.
Request timed out.
Reply from 193.137.87.15: bytes=2000 time=16ms TTL=125
Request timed out.
Request timed out.
Request timed out.
...
...
Ping statistics for 193.137.87.15:
    Packets: Sent = 56, Received = 30, Lost = 26 (47% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  16ms, Average =  2ms
```

```
Pinging srv.dq.ua.pt [193.136.83.1] with 2000 bytes of data:
Reply from 193.136.83.1: bytes=2000 time=16ms TTL=253
Reply from 193.136.83.1: bytes=2000 time=16ms TTL=253
Request timed out.
Reply from 193.136.83.1: bytes=2000 time<10ms TTL=253
Reply from 193.136.83.1: bytes=2000 time<10ms TTL=253
Reply from 193.136.83.1: bytes=2000 time<10ms TTL=253
Reply from 193.136.83.1: bytes=2000 time=16ms TTL=253
Request timed out.
Reply from 193.136.83.1: bytes=2000 time<10ms TTL=253
Reply from 193.136.83.1: bytes=2000 time<10ms TTL=253
Reply from 193.136.83.1: bytes=2000 time<10ms TTL=253
Request timed out.
Reply from 193.136.83.1: bytes=2000 time<10ms TTL=253
Reply from 193.136.83.1: bytes=2000 time<10ms TTL=253
Reply from 193.136.83.1: bytes=2000 time<10ms TTL=253
Request timed out.
...
...
Ping statistics for 193.136.83.1:
    Packets: Sent = 56, Received = 50, Lost = 6 (11% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  20ms, Average =  5ms
```

Figura 5.11 – Resultado de pings efectuados, a partir do CIC, a sistemas em vários pontos da rede.

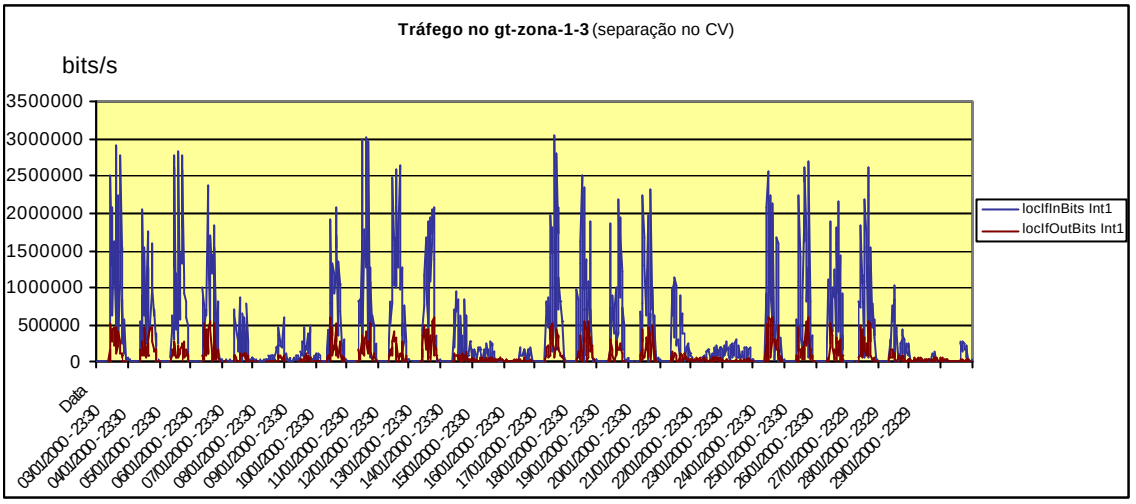


Figura 5.12 – Tráfego no gt-zona-1-3 sem utilizar o FDDI.

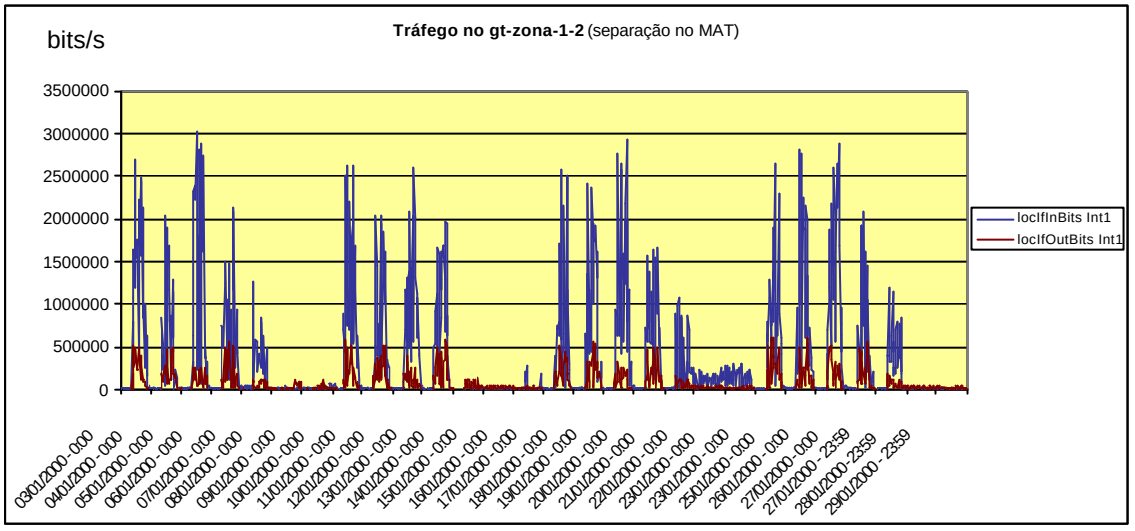


Figura 5.13 – Tráfego no gt-zona-1-2 sem utilizar o FDDI.

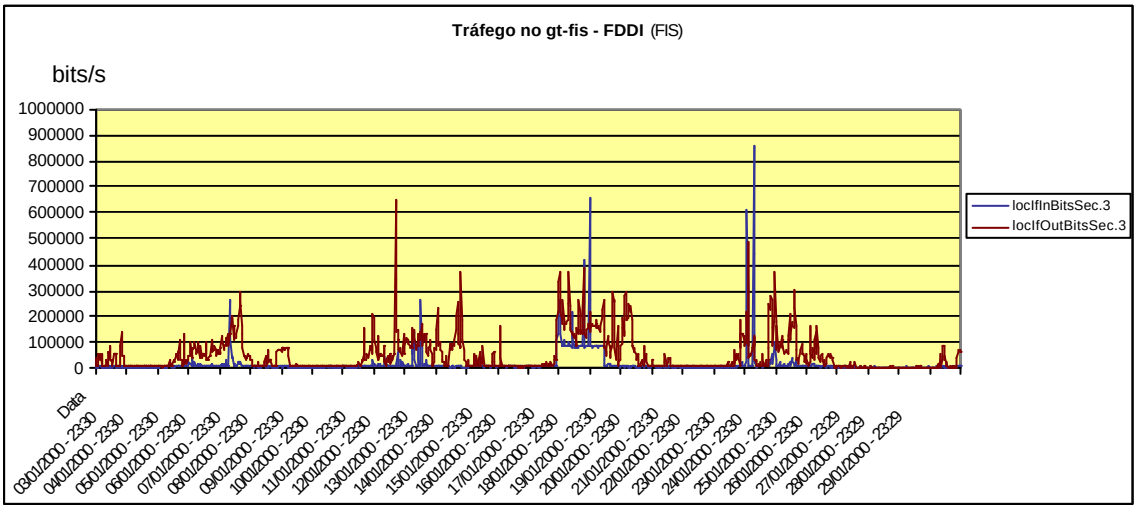


Figura 5.14 – Tráfego no gt-fis a servir apenas o Departamento de Física.

Observando os resultados anteriores verificámos que a infra-estrutura Ethernet tem uma utilização diária que chega até aos 5Mbps para o tráfego de entrada e saída, com testes de conectividade onde as perdas de pacotes chegam a valores de 30% e 40%, enquanto o FDDI tem uma ocupação que não chega nunca a 1Mbps. As razões para a perda de pacotes poderão ser várias incluindo mau funcionamento dos equipamentos, más condições do cabo, tráfego elevado, etc. Os valores apresentados evidenciam um subaproveitamento do FDDI enquanto que a infra-estrutura Ethernet se começa a atingir a saturação.

No seguimento destas constatações foi revista a organização da infra-estrutura, tendo-se procedido aos trabalhos necessários para, com a mesma infra-estrutura, reaproveitar melhor os recursos disponíveis melhorando o desempenho da rede, ou seja utilizando melhor o FDDI. A Figura 5.15, Figura 5.16 e Figura 5.17, retiradas directamente do NNM, mostram o comportamento do tráfego nos equipamentos anteriormente analisados, depois de se reorganizar a infra-estrutura. Os gráficos permitem observar um aumento significativo da ocupação da rede FDDI em detrimento da ocupação da rede Ethernet e ao mesmo tempo verificar a entrada em funcionamento (comparação da Figura 5.16 e Figura 5.17) da rede Ethernet na ausência de conectividade através do FDDI.

Para além destes dados é também de notar um aumento significativo da utilização diária da infra-estrutura em cerca de 1,5 Mbps, o que leva a concluir, uma vez que não houve novos serviços disponibilizados, que a melhoria na qualidade da infra-estrutura levou a uma maior utilização da mesma.

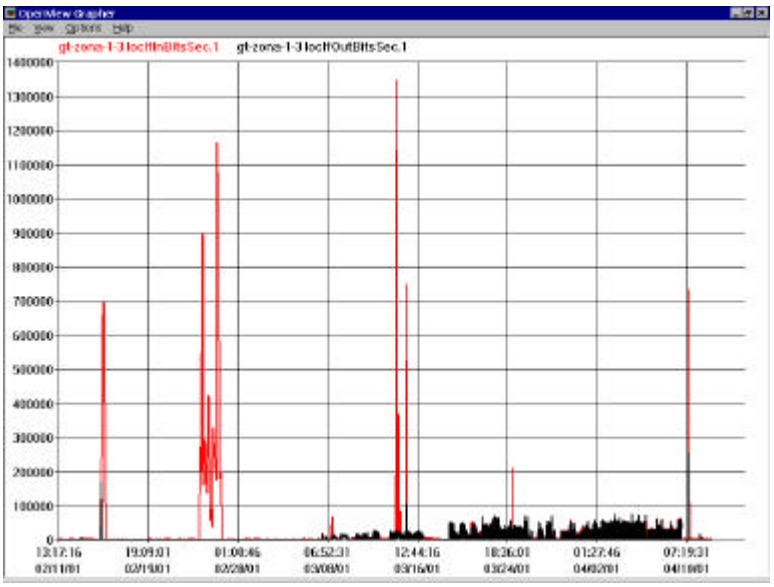


Figura 5.15 – Tráfego na Ethernet do gt-zona-1-3 utilizando o FDDI para o transporte dos dados.

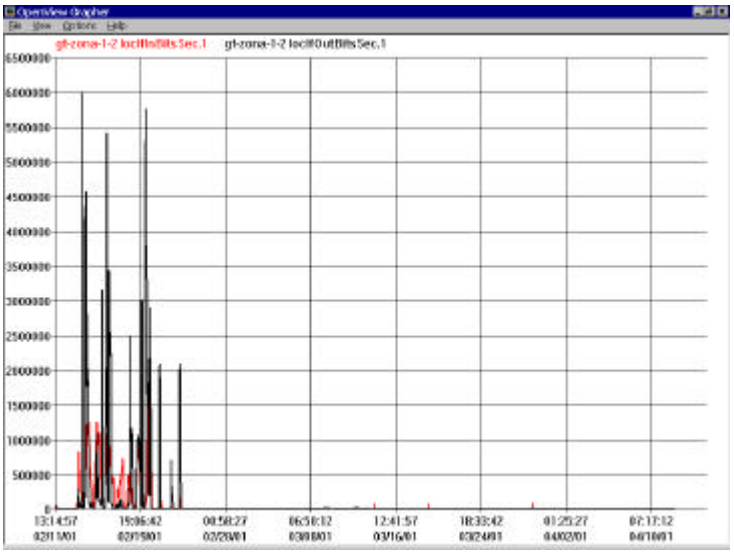


Figura 5.16 tráfego na Ethernet do gt-zona-1-2 utilizando o FDDI para transporte dos dados.

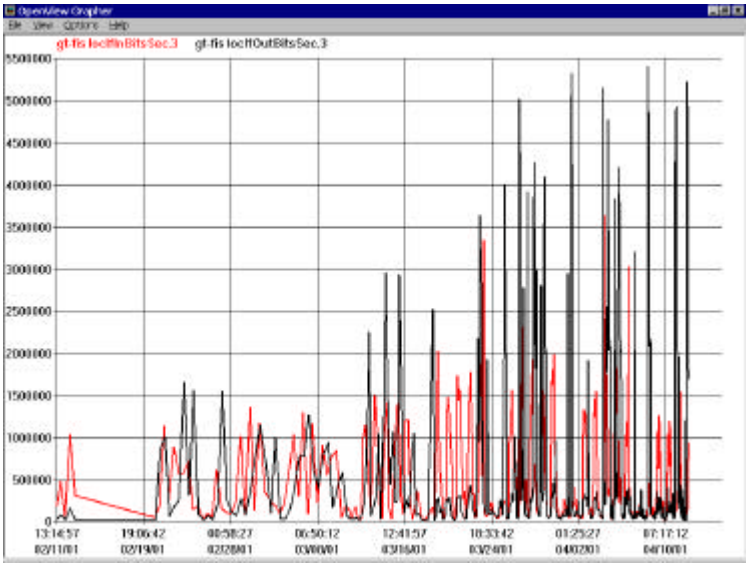


Figura 5.17 – Tráfego no FDDI do gt-fis a transportar o tráfego da zona sul.

Importava também ter uma noção do tipo de tráfego que a UA trocava com a Internet, tendo sido colocado o Observer a efectuar a monitorização da ligação de saída da UA com os resultados apresentados na Figura 5.18. Pode observar-se que o tráfego, identificado como pertencente ao Napster, ocupa cerca de 18% do total de pacotes trocados com o exterior, ou seja uma grande parte da largura de banda está a ser ocupada com tráfego originado por actividades lúdicas e não de investigação. Verificou-se também que a maior parte do tráfego trocado com o exterior é http, pelo que devem ser revistos os mecanismos de cache do proxy, afim de aferir da possibilidade de optimização que diminua o consumo de largura de banda da ligação com o exterior.

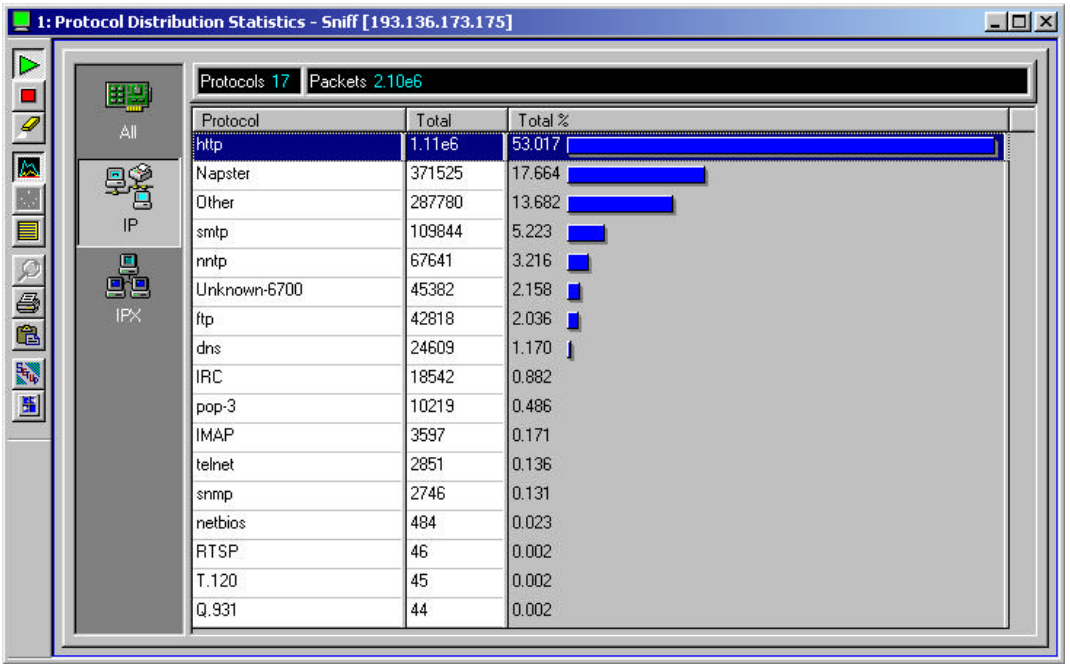


Figura 5.18 – Tipo de tráfego no acesso à Internet.

5.7 Facilidades de Configuração Remota

As várias aplicações que constituem a plataforma implementada dotaram a equipa do CIC de facilidades de configuração e gestão remota de equipamentos e computadores. São de salientar as facilidades introduzidas pelo NNM com personalização dos menus de forma a suportarem comandos predefinidos sobre os equipamentos, a possibilidade de configuração de perfis a serem aplicados a todos os equipamentos 3COM a partir do TEM e a facilidade de configuração remota de clientes e aplicações proporcionada pelo SMS.

Nesta área, e dadas a vantagens evidentes que as aplicações fornecem neste momento, é imperativo proceder à actualização do Transcend para uma versão compatível com o Windows 2000 e que suporte os novos equipamentos da 3COM, uma vez que não são disponibilizadas actualizações para esta versão há quase 2 anos. As facilidades disponibilizadas neste campo pelo SMS carecem de um estudo mais aprofundado que, por limitações de tempo, não pôde ser efectuado ao longo deste trabalho.

5.8 Inventariação de Hardware e Software

No que respeita à inventariação de equipamento, qualquer das aplicações utilizadas é capaz de o fazer. No domínio dos computadores, o SMS é sem dúvida a aplicação mais completa e que fornece a maior quantidade de informação sobre os mesmos, incluindo o hardware e o software instalado. Os relatórios disponibilizados pelo SMS concedem ao gestor a possibilidade de ter a qualquer momento o inventário completo e actualizado de toda a infra-estrutura, no que respeita a quantidades, características, versões, tipos de

equipamentos, etc. Estes relatórios podem ser criados à medida das necessidades, sendo especificados consultas à base de dados, das quais se apresenta um exemplo na Figura 5.19 e na Figura 5.20 o respectivo resultado.

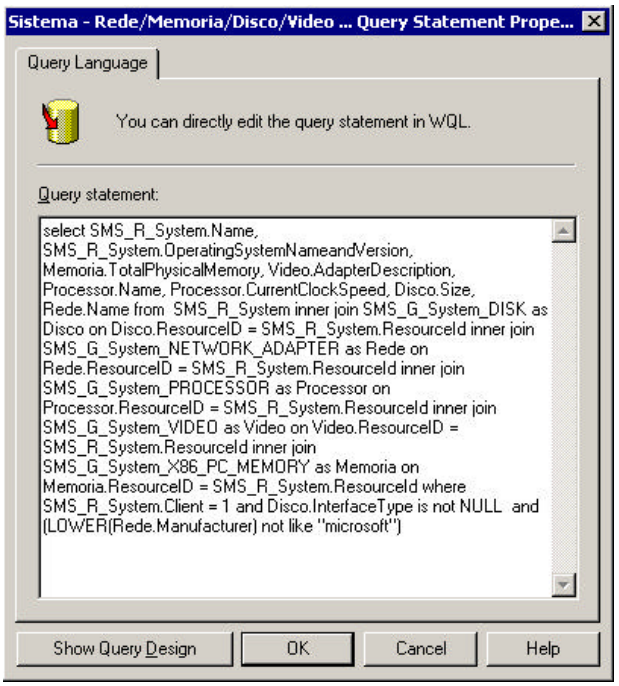


Figura 5.19 – Query em WQL.

Maquina	Sistema Operativo	Memoria (KBytes)	Placa de Video	Processador	Velocidade do Processador	Tamanho de Disco(MBytes)
SMS-CIC	Microsoft Windows NT Advanced Server 5.0	261.668		Intel Pentium II processor	450	8.675
APLICACOES	Microsoft Windows NT Server 5.0	522.476	Intel810 Video Accelerator	Unknown Intel P6 processor	731	17.359
cypress	Microsoft Windows NT Workstation 5.0	327.212	1002-4742-5C-1028-4082	Intel Pentium III or Pentium III Xeon Processor	450	6.149
ribeiro	Microsoft Windows NT Workstation 5.0	196.088	ATI 3D Rage Pro (atir3)	Intel Pentium III or Pentium III Xeon Processor	450	6.142
kalake	Microsoft Windows NT Workstation 5.0	260.332	Intel810 Video Accelerator	Unknown Intel P6 processor	865	9.538
perl	Microsoft Windows NT Workstation 5.0	392.748	1002-4742-5C-1028-4082	Intel Pentium III or Pentium III Xeon Processor	450	9.766
thunder	Microsoft Windows NT Advanced Server 5.0	523.808	Creative CT6941	Intel Pentium II processor	450	8.675
GEMINI	Microsoft Windows NT Workstation 5.0	294.256	NeoMagic Corporation	Unknown Intel P6 processor	366	6.149
relatorios	Microsoft Windows NT Advanced Server 4.0	130.484	ATI Graphics Accelerator	Intel Pentium II processor	133	4.345
celia	Microsoft Windows NT Workstation 5.0	392.744	Intel740 Video Accelerator	Intel Pentium II processor	450	8.667
servergi	Microsoft Windows NT Advanced Server 4.0	261.548	S3 Compatible Display Adapter	Intel Pentium II or Pentium II Xeon processor	400	4.345
mestrado10	Microsoft Windows NT Workstation 4.0	130.468	Intel740 Video Accelerator	Intel Pentium II or Pentium II Xeon processor	350	4.102
mestrado09	Microsoft Windows NT Workstation 4.0	130.468	Intel740 Video Accelerator	Intel Pentium II or Pentium II Xeon processor	350	4.102
mestrado08	Microsoft Windows NT Workstation 4.0	130.468	Intel740 Video Accelerator	Intel Pentium II or Pentium II Xeon processor	350	4.102
mestrado05	Microsoft Windows NT Workstation 4.0	130.468	Intel740 Video Accelerator	Intel Pentium II or Pentium II Xeon processor	350	4.102
mestrado06	Microsoft Windows NT Workstation 4.0	130.468	Intel740 Video Accelerator	Intel Pentium II or Pentium II Xeon processor	350	4.102
mestrado04	Microsoft Windows NT Workstation 4.0	130.468	Intel740 Video Accelerator	Intel Pentium II or Pentium II Xeon processor	350	4.102
mestrado02	Microsoft Windows NT Workstation 4.0	130.468		Intel Pentium II or Pentium II Xeon processor	350	4.102
mestrado01	Microsoft Windows NT Workstation 4.0	130.468	1002-474D-65-1002-0008	Intel Pentium II or Pentium II Xeon processor	350	4.102
srv-egi-gcti	Microsoft Windows NT Advanced Server 4.0	523.700	1002-4752-27-0E11-001E	Unknown Intel P6 processor	728	17.359
LULU	Microsoft Windows NT Workstation 5.0	260.332	Intel(R) 82815 Graphics Controller	Unknown Intel P6 processor	865	9.538
mestrado07	Microsoft Windows NT Workstation 4.0	130.468	Intel740 Video Accelerator	Intel Pentium II or Pentium II Xeon processor	350	4.102
pc-teste	Microsoft Windows NT Workstation 4.0	130.564	SiS 6326	Intel Pentium II or Pentium II Xeon processor	350	4.110
CD-CLONE	Microsoft Windows NT Workstation 5.0	130.596	Intel740 Video Accelerator	Intel Pentium II processor	350	4.118
CLIMA	Microsoft Windows 98	129.212	Intel(R) 810e Chipset Graphics Driver (DC133 FSB133) 4.11.01.1361	Unknown Intel P6 processor	532	6.142
GCTI02-EGI	Microsoft Windows NT Workstation 4.0	129.332	Intel815 Video Accelerator	Unknown Intel P6 processor	800	9.538
GCTI03-EGI	Microsoft Windows NT Workstation 4.0	129.332	Intel815 Video Accelerator	Unknown Intel P6 processor	800	9.538
GCTI06-EGI	Microsoft Windows NT Workstation 4.0	129.332	Intel815 Video Accelerator	Unknown Intel P6 processor	800	9.538
GCTI09-EGI	Microsoft Windows NT Workstation 4.0	129.332	Intel815 Video Accelerator	Unknown Intel P6 processor	800	9.538
GCTI05-EGI	Microsoft Windows NT Workstation 4.0	129.332	Intel815 Video Accelerator	Unknown Intel P6 processor	800	9.538
GCTI04-EGI	Microsoft Windows NT Workstation 4.0	129.332	Intel815 Video Accelerator	Unknown Intel P6 processor	800	9.538
GCTI08-EGI	Microsoft Windows NT Workstation 4.0	129.332	Intel815 Video Accelerator	Unknown Intel P6 processor	800	9.538
ASAS2	Microsoft Windows NT Workstation 5.0	196.140	1002-4742-5C-1028-4082	Intel Pentium III or Pentium III Xeon Processor	450	6.149
GCTI07-EGI	Microsoft Windows NT Workstation 4.0	129.332	Intel815 Video Accelerator	Unknown Intel P6 processor	800	9.538
GAQAP02.ADM	Microsoft Windows 98	130.564	Adaptador de gráficos PCI padrão (VGA)	Intel Pentium II or Pentium II Xeon processor	350	4.110

Figura 5.20 – Um dos relatórios de inventário gerado pelo SMS.

Na Figura 5.21 encontra-se um dos relatórios gerados pelo NNM no qual são identificadas as redes, segmentos e os nós que fazem parte da infra-estrutura.

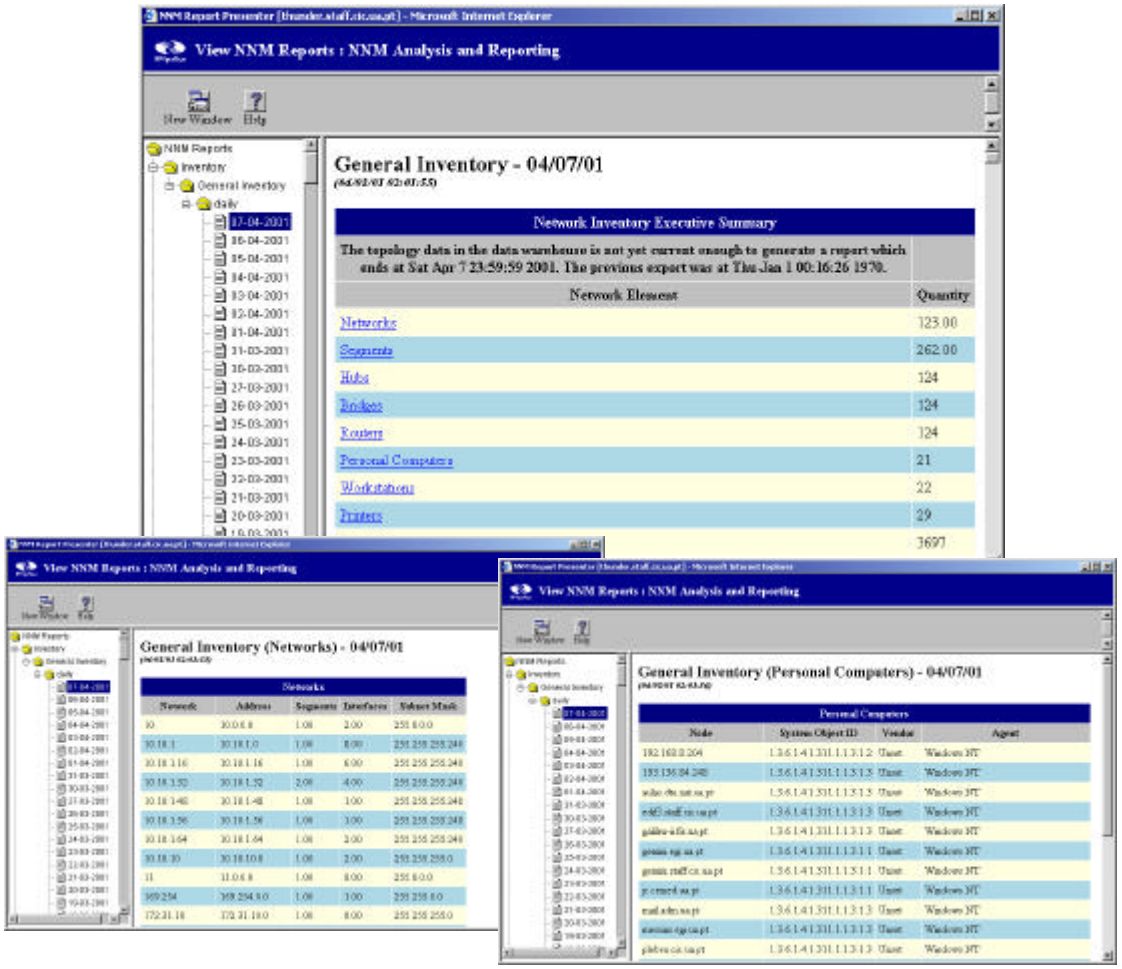


Figura 5.21 – Relatório gerado pelo NNM.

Foram verificadas as potencialidades da plataforma nesta área, faltando apenas definir objectivamente o tipo de informação que se pretende para ser utilizada para os mais diversos fins, a que está sujeito qualquer processo de inventariação.

5.9 Distribuição de Software

A distribuição de software é efectuada pelo SMS, através dos agentes instalados nos computadores clientes. A utilidade desta funcionalidade é particularmente relevante em infra-estruturas de grande dimensão, onde a instalação, por exemplo, de uma actualização do Office deixa de ser efectuada por um técnico que teria de passar por todos os computadores, com os inconvenientes inerentes a essa tarefa, como sejam a morosidade e a disponibilidade do utilizador, para passar a ser feita de uma forma centralizada sem a intervenção de ninguém.

Numa primeira fase apenas foi efectuada a distribuição do software de antivírus nos computadores do CIC (Figura 5.22) sendo agora necessário proceder à instalação dos clientes pelas restantes máquinas da UA e planear minuciosa e cuidadosamente as

distribuições que se pretendem fazer. Estes cuidados são necessários quando o universo de máquinas for alargado a toda a Universidade e um erro de configuração seja repercutido, de forma catastrófica, em toda a infra-estrutura. Neste ponto convém também referir que o processo de distribuição de software consome largura de banda, devendo ser constituídos pontos de distribuição em cada infra-estrutura local e escalonadas as instalações para horários não produtivos.

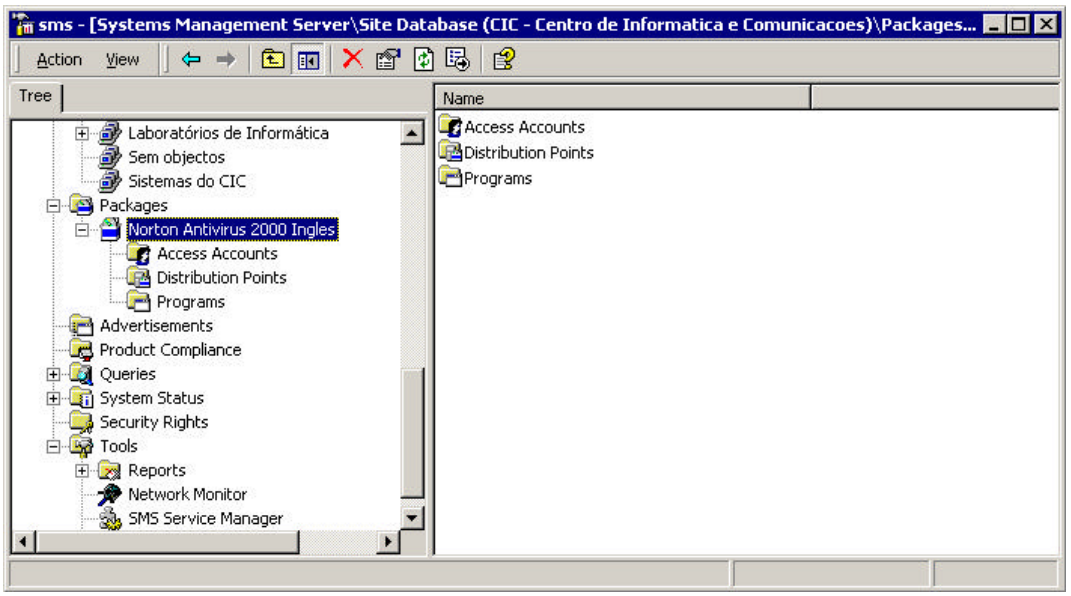


Figura 5.22 – Distribuição do pacote Antivírus.

5.10 Armazém Central de Dados

Os dados de gestão recolhidos pelas plataformas encontram-se muitas vezes em formatos proprietários, dificultando o seu acesso e tratamento estatístico. Neste trabalho foi constituído um armazém central de dados baseado num servidor Microsoft SQL 7.0, que disponibiliza um meio aberto para o desenvolvimento de aplicações de tratamento e disponibilização da informação acessível de qualquer plataforma.

O SMS guarda a informação numa base de dados SQL, utilizando e disponibilizando o acesso à mesma através de um driver ODBC WBEM, sendo as consultas efectuadas através do WQL. O NNM por sua vez também utiliza uma base de dados SQL para armazenar periodicamente a informação, disponibilizando-a para consulta através de qualquer mecanismo de acesso a bases de dados SQL.

Relativamente a este ponto, apenas foi identificada e analisada a informação armazenada nas bases de dados SQL, faltam agora especificar as consultas a implementar com base nas necessidades específicas de cada grupo.

5.11 A integração com Outras Aplicações

Entretanto e como complemento à plataforma implementada, foram utilizadas algumas aplicações de domínio público com o intuito de suprir algumas necessidades específicas.

5.11.1 SNMP4tPC nos Servidores Windows NT

Os sistemas baseados em Windows NT disponibilizam um conjunto de contadores de desempenho que são acessíveis, sem mais alterações, apenas a partir da própria máquina. O SNMP4tPC, como já foi referido, estende estas capacidades disponibilizando a informação através de SNMP, pelo que foi instalado em alguns servidores Windows NT departamentais.

A instalação do SNMP4tPC requer que o serviço SNMP esteja instalado na máquina onde será colocado o SNMP4tPC. O procedimento posterior é relativamente simples bastando trazer o pacote (disponível em [WTCS00]) e proceder à sua instalação no computador.

A instalação foi efectuada tendo em vista a recolha de variáveis relativas ao espaço em disco, ocupação de processador e memória, já que são estes os factores fundamentais no desempenho de um sistema Windows NT.

Foram configuradas colecções de dados sobre as variáveis referidas, tendo sido definidos limites a partir dos quais, os gestores são notificados, tendo em vista, mais uma vez, uma resposta tão rápida quanto possível.

5.11.2 MRTG

O MRTG surge como mais um método de visualização dos dados estatísticos apresentando numa interface Web os dados que podem ser recolhidos directamente dos equipamentos, ou retirados das bases de dados do NNM. A configuração do MRTG é relativamente simples, sendo necessário apenas instalar o pacote e adicionar o ficheiro de registo (LRF) à configuração do NNM, ficando disponível mais um menu onde se pode activar e desactivar as colecções de dados. O resultado que se obtém é apresentado na Figura 5.23, sendo todos os parâmetros do gráfico passíveis de configuração.

Do gráfico anterior, e atendendo a que esta é a porta de saída da UA, conclui-se que esta instituição é, essencialmente, consumidora de informação. Este gráfico podia ser obtido através do NNM, no entanto, era apenas acessível a partir de uma consola do NNM (Figura 5.24).

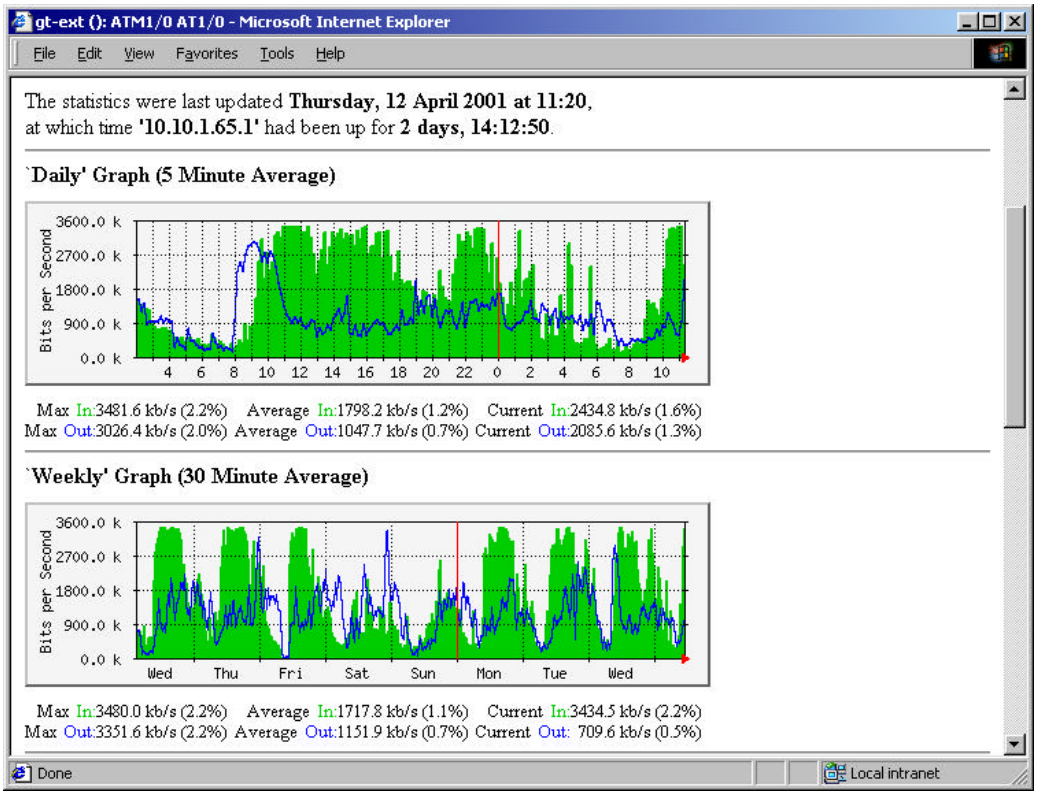


Figura 5.23 – Gráfico da ocupação da ligação à Internet (MRTG).

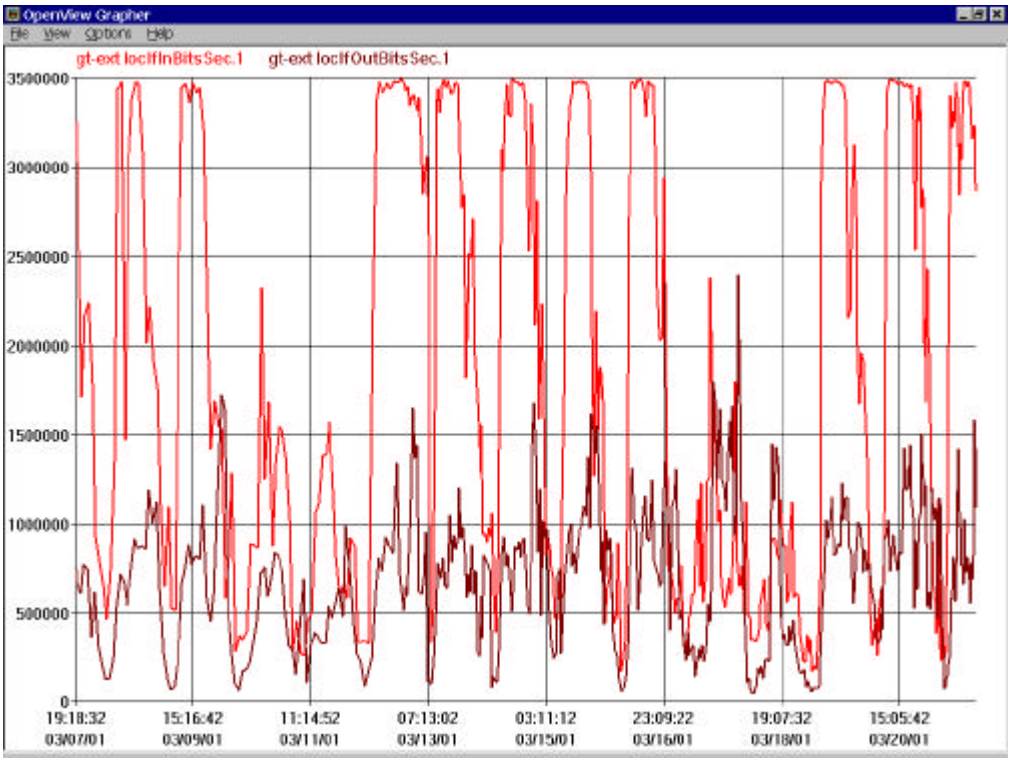


Figura 5.24 – Gráfico da ocupação da ligação à Internet (NNM).

5.12 A plataforma na Resolução de Problemas

A monitorização constante da rede previne muitos problemas e alerta atempadamente para outros, mas não elimina por completo a sua existência. No entanto, pode desempenhar um papel importante na identificação rápida de qualquer problema que surja, sendo um exemplo os casos que são apresentados de seguida, onde a plataforma protagonizou a identificação dos problemas.

5.12.1 Falta de Desempenho na Aplicação de Contabilidade UA

A infra-estrutura física da rede de dados do Edifício III alberga duas sub-redes lógicas distintas, suportadas por equipamento independente, tal como apresenta a Figura 5.25.

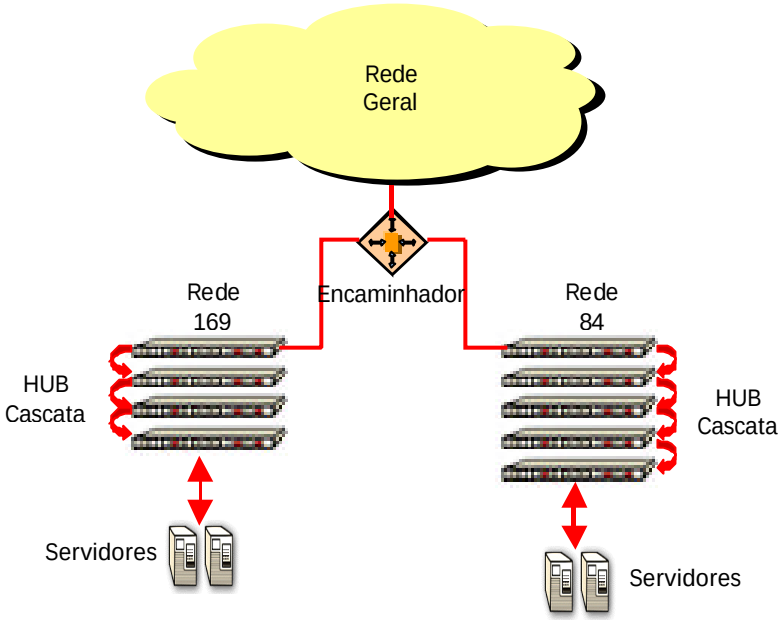


Figura 5.25 – Configuração inicial da rede da administração.

Em Maio de 2000, foram detectados problemas nas ligações à máquina da contabilidade, estando a principal dificuldade relacionada com o tempo de acesso das máquinas das secretarias das várias Unidades, à base de dados dos Serviços Financeiros da UA.

O sistema de processamento orçamental, assente numa filosofia cliente servidor, começou a apresentar vários problemas de desempenho, que, à primeira vista, pareciam ser provocados pela rede. Dado que o volume de máquinas existentes, no Edifício, era significativo e sua interligação suportada por concentradores, foi aconselhada a aquisição de um comutador Ethernet, de forma a permitir o seccionamento da rede em vários troços, com uma configuração final apresentada na Figura 5.26, onde foram configuradas duas VLANs no comutador adquirido, aproveitando deste modo o equipamento na sua totalidade.

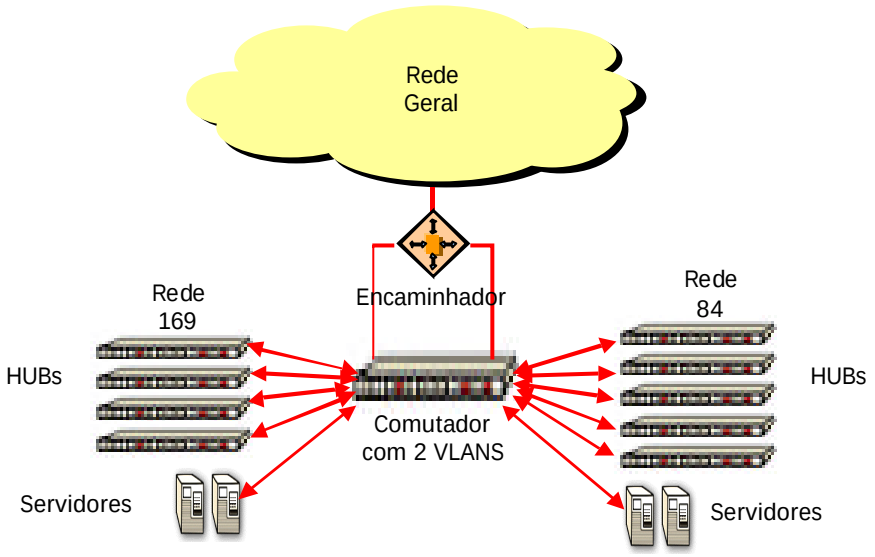


Figura 5.26 – Reorganização da rede da administração.

No entanto, mesmo depois desta configuração, os problemas persistiram, sendo efectuados de seguida algumas medições, de forma a identificar as possíveis causas.

O NNM não tinha detectado nenhum problema, quer relacionado com a rede, quer com a conectividade da máquina em questão, pelo que, foram activados mecanismos de monitorização da actividade da rede em geral e da ligação à máquina da contabilidade em particular. Os resultados, mais uma vez, foram inconclusivos na detecção de algum problema, no entanto eliminaram a possibilidade de falta de desempenho da rede, que inicialmente era apontada como sendo a origem dos problemas (a Figura 5.1 mostra a ocupação da largura de banda efectuada pela máquina da contabilidade em operação).

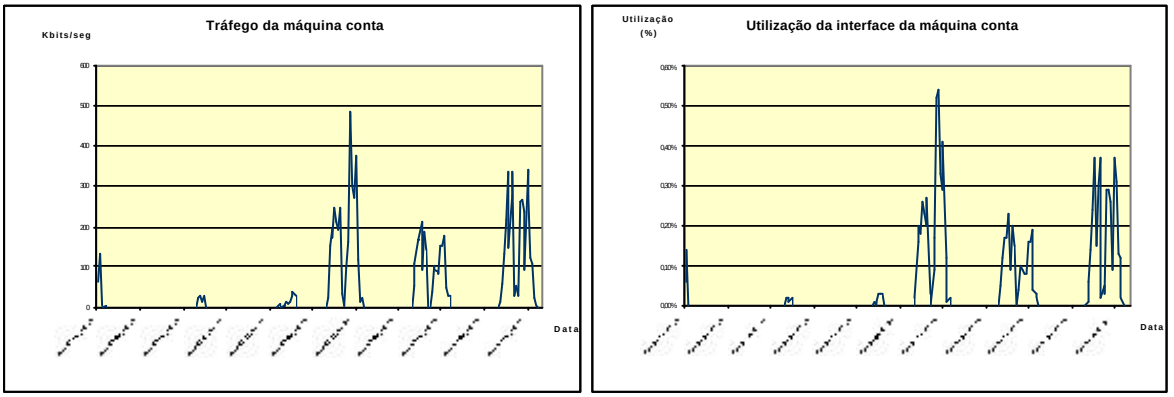


Figura 5.27 – Ocupação da interface da máquina conta obtida através do TEM.

Depois destes testes, e de ter sido excluída a rede como factor de interferência no desempenho da aplicação, foram efectuados alguns testes no servidor que suporta a BD, que revelaram falta de memória da máquina e de desempenho dos discos. Depois de resolvidas estas duas questões, as dificuldades de acesso foram eliminadas, assim como a responsabilidade da rede de dados.

5.12.2 *Falta de Conectividade da Rede Interna da Mecânica*

A infra-estrutura física do edifício da Engª Mecânica é um misto de cablagem estruturada UTP CAT5 e BUS com RG58, interligadas por um conjunto de concentradores e repetidores. A infra-estrutura descrita, que servia duas Unidades, a Mecânica e a Civil, apresentou vários problemas de conectividade interna e com a rede geral. A Figura 5.28 mostra o resultado da execução do comando ping para testar a conectividade com o servidor.

```
Pinging srv.mec.ua.pt [193.137.85.1] with 2000 bytes of data:
Reply from 193.137.85.1: bytes=2000 time=16ms TTL=253
Reply from 193.137.85.1: bytes=2000 time=16ms TTL=253
Request timed out.
Reply from 193.137.85.1: bytes=2000 time<10ms TTL=253
Reply from 193.137.85.1: bytes=2000 time<10ms TTL=253
Request timed out.
Reply from 193.137.85.1: bytes=2000 time=16ms TTL=253
Request timed out.
Request timed out.
Request timed out.
Reply from 193.137.85.1: bytes=2000 time<10ms TTL=253
Request timed out.
Reply from 193.137.85.1: bytes=2000 time<10ms TTL=253
Reply from 193.137.85.1: bytes=2000 time<10ms TTL=253
Reply from 193.137.85.1: bytes=2000 time<10ms TTL=253
Request timed out.
...
...
Ping statistics for 193.137.85.1:
    Packets: Sent = 56, Received = 29, Lost = 27 (48% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  20ms, Average =  5ms
```

Figura 5.28 – Resultado do teste de conectividade efectuado ao servidor da Mecânica.

Depois de uma análise à rede e à sua interligação física, que por não corresponder à normalização implementada na UA necessitou de algum tempo para se perceber o que liga a quê, concluiu-se que existiam demasiados troços Ethernet, sendo necessário proceder à sua separação física (Figura 5.29).

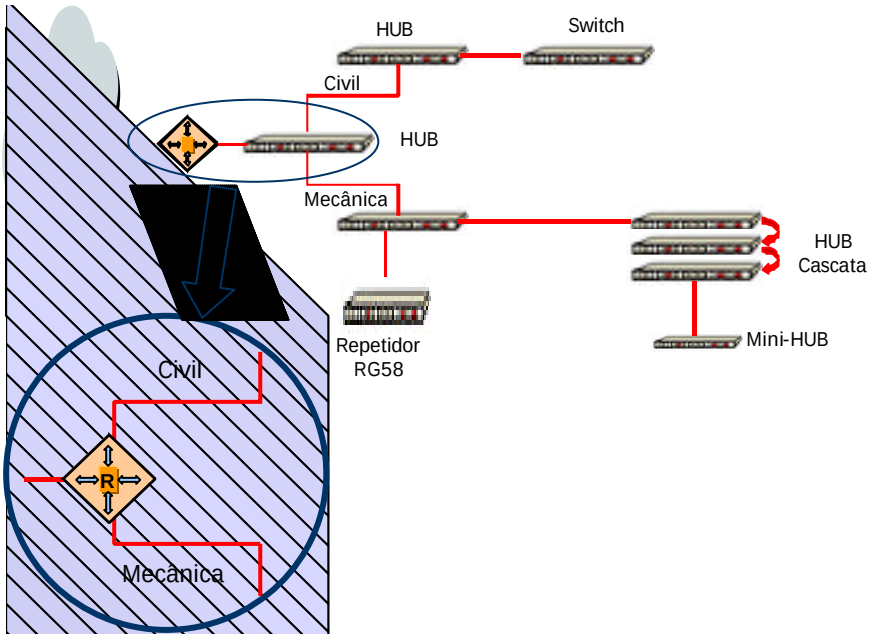


Figura 5.29 – Configuração física da infra-estrutura de informática do Edifício da Mecânica.

Na separação dos troços optou-se por isolar as redes das duas Unidades, ficando a configuração final como a que se apresenta na Figura 5.29.

Depois dos procedimentos de separação, os problemas persistiram e, aliado ao facto de nenhum dos equipamentos constituintes da rede possuir facilidades de gestão, foi necessário colocar equipamento de monitorização com o objectivo de identificar a causa dos problemas.

O Observer, foi a solução de software preferida para efectuar a monitorização da rede, tendo ficado em monitorização durante cerca de uma semana. Após este período de monitorização, não foram detectadas causas que justificassem as perturbações sentidas na rede. Os únicos problemas detectados resumiram-se a períodos utilização da rede entre os 40% e 70%, que não justificam as percas de pacotes verificadas na comunicação com as máquinas da rede.

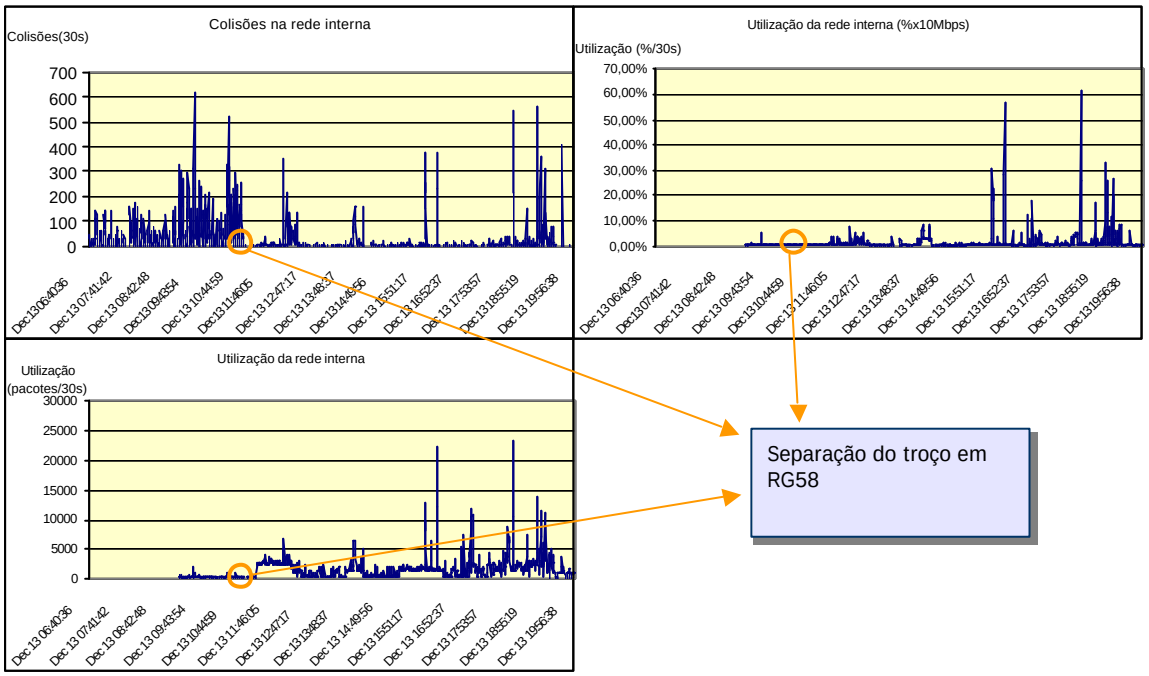


Figura 5.30 – Gráficos de utilização e erros no troço da Mecânica.

Seguidamente a estes testes, optou-se por seccionar a rede da Mecânica em segmentos separados por um comutador 3COM, dotado de capacidades de gestão, sendo ocupadas 3 portas do comutador, uma com o encaminhador, outra com a rede do 3º piso e a última com a rede do R/Ch e do 2º Piso. Detectou-se que os erros ocorriam na sua maioria no troço do R/Ch, tendo sido desligado o troço em cablagem RG58 o que provocou a diminuição das condições de erros, como se encontra retratado na Figura 5.30. No entanto, os problemas não se resolveram todos, uma vez que aleatoriamente ocorriam demasiadas

colisões, tendo sido diagnosticado um mau contacto de uma das tomadas de rede que, depois de desligada, resolveu de vez os problemas da rede.

Na sequência de todos estes trabalhos aconselhou-se o Departamento de Mecânica a aquisição de um comutador Ethernet tendo em vista dois objectivos, o primeiro minorar a propagação dos erros por toda a rede, seccionando-a em segmentos, a segunda baixar os picos de utilização verificados na rede.

5.12.3 Falta de Conectividade na Rede Interna do CEFASI

A rede interna do CEFASI apresentou recentemente problemas que originaram a quebra da comunicação internamente e também para a rede geral.

Depois de alertados para o problema, através do NNM, da constante alternância do estado da porta do encaminhador entre acessível e inacessível e também da falta de conectividade entre a estação de gestão e o servidor local do Departamento, efectuaram-se vários testes que visaram a detecção do problema. A infra-estrutura é baseada em cablagem estruturada CAT5 e certificada, no entanto os equipamentos activos que a constituem são do tipo concentrador, existindo ligações a mini-concentradores dispersos pelos laboratórios de informática, com a configuração apresentada na Figura 5.31.

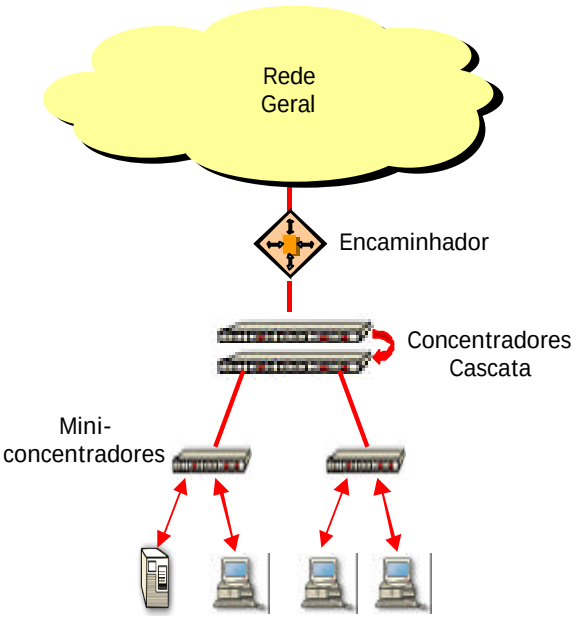


Figura 5.31 – Configuração interna da rede do CEFASI.

Os equipamentos que constituem esta rede não apresentam facilidades de gestão, no entanto o conhecimento da sua configuração física e o conhecimento do historial da rede, podem indicar possíveis caminhos para a solução do problema. O servidor de rede, baseado em Novell, há já bastante tempo que apresentava problemas de hardware e nos dias em que os problemas de rede se intensificaram o servidor encravou várias vezes e sempre que era desligado os problemas de conectividade desapareciam. Ora aqui estava

uma causa provável para o problema. No entanto, depois de desligado completamente o servidor, da rede, os problemas voltaram a aparecer com a mesma persistência.

Posto isto, foi necessário voltar à estaca zero e proceder a uma nova análise da situação, partindo para a segunda hipótese possível, que era o possível mal funcionamento dos mini-concentradores dos laboratórios. O problema era realmente de um destes concentradores que foi substituído, ficando a rede a funcionar de novo normalmente.

6 Conclusões e Trabalho Futuro

Com a crescente dependência de todos os serviços e áreas de negócio das infra-estruturas de informática, deposita-se nas tecnologias e soluções de gestão a difícil tarefa de assegurar o funcionamento permanente dessas infra-estruturas. A gestão é uma área muito abrangente, na qual existem inúmeras soluções e tecnologias que respondem aos mais diversos requisitos, dificultando a escolha da solução "ideal" para cada caso.

O presente trabalho restringiu-se apenas ao estudo de mecanismos e soluções de gestão de redes e sistemas, tendo ficado de fora muitas outras áreas que importa cuidar nas actuais infra-estruturas de informática, entre elas a gestão de armazenamento e de segurança.

No desenvolvimento operacional do trabalho são várias as conclusões a retirar, importando mencionar que a gestão efectiva não depende apenas do estudo e implementação de plataformas de gestão, mas é em grande parte constituída por um conhecimento profundo, quer das tecnologias envolvidas, quer da organização física e lógica da infra-estrutura, complementada com muito tempo e dedicação na análise e exploração das várias situações que ocorrem ao longo do tempo. Também se concluiu que os resultados, obtidos com diferentes ferramentas, podem apresentar uma grande disparidade entre si, ficando este facto a dever-se às implementações das normas, pelos diferentes fabricantes. A documentação publicada pelos fabricantes sobre as implementações efectuadas nos seus equipamentos é muitas vezes extremamente pobre, dificultando o entendimento das funcionalidades e facilidades desses equipamentos.

No que respeita aos utilizadores, mesmo sem dados concretos para apresentar, e baseado apenas na experiência profissional, pode-se afirmar que a maioria dos problemas reportados se relaciona com o desconhecimento na utilização ou funcionamento dos serviços, aplicações e sistemas.

Os objectivos que nortearam o desenvolvimento da presente dissertação foram cumpridos na generalidade, tendo sido implementada uma plataforma de gestão de redes e sistemas já com provas dadas da eficácia e da necessidade destas soluções. O estudo e implementação aqui efectuados, poderão servir como base para a constituição de uma plataforma de gestão a aplicar numa infra-estrutura com os mesmo requisitos da infra-estrutura da Universidade de Aveiro, que pela diversidade de tecnologias e sistemas potenciou um estudo bastante alargado das ferramentas de gestão

Este trabalho serviu, entre muitas outras coisas, para adquirir e solidificar conhecimentos na área da gestão de redes e sistemas, tendo sido mantido um contacto muito estreito com o que de mais recente se faz e investiga nestas áreas. Em complemento foram adquiridos um conjunto de conhecimentos que permitem, agora, encarar a gestão com outra perspectiva, valorizando muitos outros factores para além da plataforma de gestão.

Considero que este trabalho foi só um começo e um adquirir de conhecimentos que permitirão, de um modo mais profissional, implementar e adequar uma solução de gestão às necessidades de cada caso em concreto.

No que respeita a evoluções futuras e como continuação do presente trabalho, coloca-se agora uma nova etapa que passará pela generalização da utilização da plataforma implementada, no âmbito da gestão da infra-estrutura de informática da Universidade de Aveiro e a actualização das aplicações de modo a responderem às novas exigências que entretanto se apresentaram. As vantagens e benefícios da utilização da plataforma são reais e encontram-se enumerados ao longo da dissertação, que também inclui um estudo de implementação na referida infra-estrutura.

Acrónimos

ARPA	Advanced Research Projects Agency
API	Application Programmable Interface
ARF	Application Registration File
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
CATV	Community Antenna Television / Cable Antenna Television
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CET	Centro de Estudos de Telecomunicações
CIM	Common Information Model
CMIP	Common Management Information Protocol
CMOT	CMIP sobre TCP/IP
COP	Centro de Operações
CORBA	Common Object Request Broker Architecture
DEN	Directory Enabled Network
DHCP	Dynamic Host Configuration Protocol
DMI	Desktop Management Interface
DMTF	Desktop Management Task Force
DNS	Domain Name System
DoD	Department of Defense
FDDI	Fiber Distributed Data Interface
FIRST	Fiber in the Residential Subscriber Terminal
HMP	Host Monitoring Protocol
HTTP	HyperText Transfer Protocol
IAB	Internet Arquitecture Board
ICMP	Internet Control Message Protocol
IEEE	Institute of Electric and Electronic Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JMAPI	Java Management API
JMX	Java Management Extensions
LAN	Local Area Network
LB	Largura de Banda
LDAP	Lightweight Directory Access Protocol
LFR	Local Registration File
MI	Management Interface
MIB	Management Information Base
MIF	Management Information Format
MSP	Management Service Provider
NNM	Network Node Manager
ONU	Optical Network Unit
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

ovw	OpenView Windows
PVC	Permanent Virtual Circuit
RF	Radio Frequência
RFC	Request for Comments
RIS	Remote Installation Services
RMON	Remote Monitoring
SGMP	Simple Gateway Management Protocol
SMS	Systems Management Server
SNMP	Simple Network Management Protocol
SNMPv2	Simple Network Management Protocol versão 2
SNMPv3	Simple Network Management Pr otocol versão 3
SP	Service Provider
SVC	Switched Virtual Circuit
TI	Tecnologia da Informação
TMN	Telecommunication Management Network
TV	Televisão
UA	Universidade de Aveiro
USM	User Security Model
VCAM	View-based Access Control Model
WBEM	Web Based Enterprise Management
WLRF	Web Launcher Registration File
WMI	Windows Management Instrumentation
WQL	WMI Query Language
XML	Extended Markup Language

Referências

[ARA00a] Audrey Rasmussen, " Network Directory Management", *Network World Fusion*, Set. 2000.

[ASC00a] Amy Schurr, "Introducing a new Kind of service provider: the MSP", *Network World Fusion*, Fev. 2000.

[AWI01] Art Wittman, " HP Reinvents Itself – Again", Network Computing, Fev. 2001.

[BBR00] Big Brother, "the big brother system and network monitor" *"http://www.bb4.com/features.html"*, 2000

[BGO99] Barb GoldWorm, "From software to services – making management work", Network World Fusion, Set. 1999.

[CAI01a] Computer Associates International, "Unicenter TNG Framework Version 2.1 Technical Overview", *Computer Associates*, 2001.

[CAI01b] Computer Associates International, "Unicenter TNG Total Enterprise Management Overview", *Computer Associates*, 2001.

[CIS00] Cisco Systems, "CiscoWorks 2000", http://www.cisco.com/warp/public/cc/pd/wr2k/, 2000.

[CJD97] C. J. Date, "A guide to the SQL standard: a user's guide to the standard database SQL", *Addison-Wesley*, 1997.

[CRN01] CRN Test Center, "Windows 2000 Server, Professional Pair Eases Client Management", TechReviews, Fev. 2001.

[DDR00] Dennis Drogseth, "Inventory Management as Rorschach test", *Network World Fusion*, Out. 2000.

[DMA00] Darren Mar-Elia, "Leveraging Windows Management Instrumentation in Win2k Pro", Windows 2000 Magazine, Mar. 2000.

[DMTF98] DMTF Technical Committee, "Desktop Management Interface Specifications – Version 2.0s", *DMTF*, Jun. 1998.

[DMTF01a] DMTF, "Distributed Management Task Force (DMTF) Membership List", *http://www.dmtf.org/db/list/company.php3*, 2001.

[DTP99] David T. Perkins, "RMON Remote Monitoring of SNMP-Managed LANs", *Prentice Hall*, 1999.

[ERP99] Edwin E. Mier, Robert J. Smithers Jr., Peter C. Hugger, " Which Switch Manages Best?", *Business Communications Review*, Mar. 1999.

[GKO95] George Koch, "Oracle: the complete reference 3rd ed", *McGraw-Hill*, 1995.

[HIT99] Hitachi, "IT Layers White Paper", *Hitachi Software Engineering America*, 1999

[HKG97] Jill Huntington-Lee, Kornel Terplan, Jeff Gibson, "HP OpenView, A Manager's Guide", *McGraw-Hill Series*, 1997.

[HPOV00a] HP OpenView, "integration with ecs"", *http://www.openview.hp.com/*, 2000.

[HPOV00b] HP OpenView, "HP OpenView Portfolio Partners with Certified Applications", http://ovweb3.external.hp.com/solcat/products/certified.cfm, 2001.

[HSB99] H. Hegering, Sbastian Abeck, Bernard Neumair, "Integrated Management of Networked Systems", *Morgan Kaufmann*, 1999.

[IDC00a] IDC, "Network Meets System Management", *http://www.idc.com - International Data Corporation*, Jan. 2000.

[IETF] Internet Engineering Task Force, *http://www.ietf.org*

[JAB96] Jorge Abreu, "Redes de Televisão por Cabo Situação Actual e Perspectivas de Evolução Futura ", *Dissertação de Mestrado-DETUA*, 1996.

[JHE99] James Herman, "The Impact of Ebusiness on Enterprise IT Management", *Business Comunications Review*, Out. 1999.

[JHI00] John Hidalgo, "Introduction to Directory Enabled Networks (DEN) ", *DMTF 2000 Developers Conference*, Jun.2000.

[JJA98] J. Jacobson, "Security Comes to SNMP: The New SNMPv3 Proposed Standards", *Cisco – The Internet Protocol Journal*, Dez. 1998.

[JTU00] Jim Turner, "The DMTF Harnessing the Internet Tomado", *DMTF Annual Conference 2000*, Jun. 2000.

[KSS00] Karanjit S. Siyan, " Network Management for Microsoft Networks Using SNMP", *Microsoft Technet*, 1999.

[MAR00] Marconi, "ServiceOn Foundation 1.1 - Carrier Class Network Management Solution for Broadband Networks", *Marconi*, Jun. 2000.

[MMSM00] Mike Martin, Marc Songini, "Management Service Providers Unite", Network World Fusion, Ago. 2000.

[MCS99a] Microsoft Consulting Services, "MS Systems Management Server Deployment Project Plan", *Microsoft Corporation*, Fev. 1999.

[MRU00] Mark Russinovich " Inside Windows Management Interface", Windows 2000 Magazine, Jan. 2000.

[MSC97a] Microsoft Corporation, "Microsoft Systems Management Server Installer", *Microsoft Corporation*, Mai. 1997.

[MSC99a] Microsoft Corporation, "Planning, Deploying and Managing MS Windows 2000 with Systems Management Server 2.0 – Technical Notes", *Microsoft Technet*, Fev. 1999.

[MSC99b] Microsoft Corporation, "Systems Management Server 2.0 Server Sizing in an Organization", *Microsoft Technet*, Ago. 1999.

[MSC99c] Microsoft Corporation, "Advanced Systems Management Server 2.0 Reporting", *Microsoft Technet*, Ago. 1999.

[MSC99d] Microsoft Corporation, "Windows Installer Service Overview", *Microsoft Corporation*, 1999.

[MSC00a] Microsoft Corporation, "Implementing Directory Enabled Networks Using Windows 2000 Technology", *Microsoft Technet*, Abr. 2000.

[MSC00b] Microsoft Corporation, "Introduction to Windows 2000 Management Services White Paper", *Microsoft*, Abr. 2000.

[MSC00c] Microsoft Corporation, "Windows Management Instrumentation: Platform SDK", *Microsoft Help*, 2000.

[MSC00d] Microsoft Corporation, "Windows 2000 Desktop Management", *Microsoft*, Abr. 2000.

[MSC01a] Microsoft Corporation, "Introducing Systems Management Server Version 2.0", *Microsoft TechNet*, Fev. 2001.

[MSC01b] Microsoft Corporation, "Creating Your SMS Security Strategy", *Microsoft TechNet*, Fev. 2001.

[NIT00] Network Instruments, "Observer Suite User Guide", *Network Instruments*, 2000.

[NNM00a] Hewlett Packard, "Runtime Release Notes for Windows NT", *Hewlett Packard*, Fev. 2000.

[NNM00b] Hewlett Packard, "DevKit Release Notes for Windows NT", *Hewlett Packard*, Fev. 2000.

[NNM00c] Hewlett Packard, "Quick Start Installation Guide for Windows NT", *Hewlett Packard*, Fev. 2000.

[NNM00d] Hewlett Packard, "A Guide to Scalability and Distribution", *Hewlett Packard*, Fev. 2000.

[NNM00e] Hewlett Packard, "Reporting and Data Analysis", *Hewlett Packard*, Fev. 2000.

[NNM00f] Hewlett Packard, "Configuring Customer-Specific Network Management", *Hewlett Packard*, Fev. 2000.

[NNM00g] Hewlett Packard, "Creating and Using Registration Files", *Hewlett Packard*, Fev. 2000.

[NNM00h] Hewlett Packard, "Managing Your Network", *Hewlett Packard*, Fev. 2000.

[NNM00i] Hewlett Packard, "Migration Guide", *Hewlett Packard*, Fev. 2000.

[NNM00j] Hewlett Packard, "Integration Concepts", *Hewlett Packard*, Fev. 2000.

[NNM00k] Hewlett Packard, "Application Style Guide", *Hewlett Packard*, Fev. 2000.

[NNM00l] Hewlett Packard, "OVW Developer's Guide", *Hewlett Packard*, Fev. 2000.

[NNM00m] Hewlett Packard, "SNMP Developer's Guide", *Hewlett Packard*, Fev. 2000.

[NNM00n] Hewlett Packard, "Java Developer's Guide", *Hewlett Packard*, Fev. 2000.

[NNM00o] Hewlett Packard, "Windows NT User Reference Pages", *Hewlett Packard*, Fev. 2000.

[NNM00p] Hewlett Packard, "Integrating HP OpenView Network Node Manager 6.1 and Microsoft Terminal Server", *Hewlett Packard*, Fev. 2000.

[NWC00a] Network World Computing, "Complete Buyer's Guide WAN Analysers/Probes", *Interactive Buyer's Guide*, Out. 2000;

[NWI00] NerveWire, "Investing in Desktop Management Productivity", *NerveWire, Inc*, Jun. 2000.

[NWF01a] NetworkWorldFusion, "NetworkWorldFusion Interactive Buyers Guide", *NetworkWorldFusion*, Jan. 2001.

[ONG706] Open Group Technical Standard, "DCE 1.1: Remote Procedure Call - Document Number C706", *The Open Group*, Ago. 1997.

[PMO00] Peter Morrissey, " Distributed Analysers: The Next Best Thing", Network Computing, Out. 2000.

[RCW00] Raymond C. Williams, "DMTF Technical Roadmap for Enterprise Management for e-business in the 21st Century", *DMTF Annual Conference 2000*, Jun. 2000.

[RSJ98a] Ricardo T. Martins, Sérgio Bernardo, José Luís Oliveira, "Interface de Gestão Web para HP OpenView", *Electrónica e Telecomunicações – Revista do DETUA*, Vol. 2, Nº 2, pg. 373-380, Jan. 1998.

[RSJ98b] Ricardo T. Martins, Sérgio Bernardo, José Luís Oliveira, "NetAdmin – Interface Web para HP OpenView", *Conferência Redes de Computadores*, Nov. 1998.

[SEL99] Susan Ellerin, "Network management platforms make the grade", *NetworkWorld*, Set. 1999.

[SUN99a] SUN Microsystems, "JAVA™ Management Extensions White Paper", *SUN Microsystems*, Jun. 2000.

[SUN00a] SUN Microsystems, "JAVA™ Management Extensions Instrumentation and Agent Specification, v1.0", *SUN Microsystems*, Jul. 2000.

[SUN00b] SUN Microsystems, "SolsticeTM Site ManagerTM 2.3 A Technical White Paper", *http://www.sun.com/software/white-papers/wp-site.domain.mgr/index.html*, 2000.

[SUN00c] SUN Microsystems, "Solstice Cooperative ConsolesTM", *http://www.sun.com/software/cc/ds-cc/*, 2000.

[TCO00a] Todd Coopee, "Desktop Management Suite RFP", *NetworkWorldFusion*, Jan. 1999.

[TEM97a] 3COM, "Transcend Network Administration Guide", *3COM Press*, 1997.

[TEM97b] 3COM, "Transcend Network Enterprise VLAN Manager User Guide", *3COM Press*, 1997.

[TOE00] Tobias Oetiker, "Multi Router Traffic Grapher", *http://people.ee.ethz.ch/~oetiker/webtools/mrtg/*, 2000.

[TPA99] Toni Paila, "The Security of Network Management", *Department of Computer Science – Helsinki University of Technology*, Nov. 1999.

[UA99] Universidade de Aveiro, "Guia da Universidade de Aveiro 1999/2000", *Universidade de Aveiro*, Out. 1999.

[VER00] Veritas Corporation, "Veritas WinINSTALL LE – Reference Manual", *http://seer.support.veritas.com/docs/229402.htm, 2000.*

[VRG99] Victor R. Garza, "NNM 6.0 adds impressive functionality, customizable Web interface", *InfoWorld*, Mar. 1999.

[WBU00] Winston Bumpus, "The DEN-CIM Connection: A Roadmap to Directory-Enabled Networks", *DMTF 2000 Developers Conference*, Jun. 2000.

[WST98] William Stallings, "SNMPv3: A Security Enhancement for SNMP", *IEEE Communications Surveys*, Vol.1, No.1, quarto trimestre 1998.

[WST99] William Stallings, "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2 Third Edition", *Addison Wesley*, 1999.

[WTCS00] Williams Technology Consulting Services, "SNMP4tPC", *http://www.wtcs.org/snmp4tpc/*