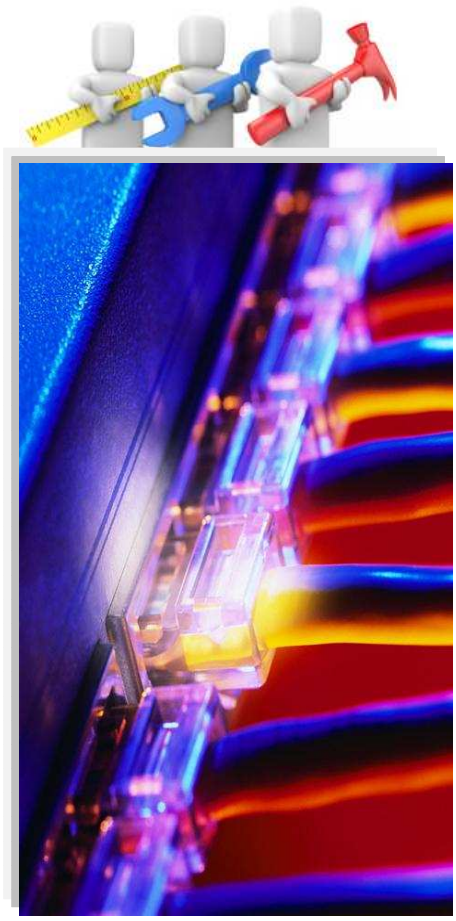
Universidade de Aveiro
2009
Departamento de Electrónica, Telecomunicações e Informática

Hermano Filipe Domingues Pereira

Avaliação de ferramentas de monitorização e gestão de redes



Universidade de Aveiro
2009
Departamento de Electrónica, Telecomunicações e Informática

Hermano Filipe Domingues Pereira

Avaliação de ferramentas de monitorização e gestão de redes

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 Professor Doutor Paulo Ferreira, Professor Auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e sob a co-orientação do Professor Doutor António Nogueira, Professor Assistente do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

O júri

Presidente

Prof. Dr. Paulo Miguel Nepomuceno Pereira Monteiro
Universidade de Aveiro

Prof. Dr. Joel José Puga Coelho Rodrigues
Departamento de informática da Faculdade de Engenharia da Universidade da Beira Interior

Prof. Dr. Paulo Jorge Salvador Serra Ferreira
Universidade de Aveiro

Prof. Dr. António Manuel Duarte Nogueira
Universidade de Aveiro

agradecimentos

A todos os que foram agentes facilitadores durante o desenvolvimento deste exigente processo e fizeram parte dele, directa ou indirectamente.

À família, que é imprescindível e insubstituível, nestes momentos, e que me acompanha, motiva e compreende, ajudando sempre.

Ao pessoal do CICUA que demonstrou disponibilidade, capacidade de inter-ajuda, facultando apoio técnico, partilha de conhecimento e momentos de crescimento profissional.

Aos amigos que existem para todas as ocasiões, agradeço o apoio incondicional, o altruísmo, a amizade.

Aos professores Paulo Jorge Salvador Serra Ferreira e António Manuel Duarte Nogueira, meus orientadores, por todo o empenho, sabedoria, compreensão e pelas discussões e sugestões que levaram à conclusão desta dissertação.

À minha esposa, Eunice, por todo o amor, dedicação e motivação que me concedeu, iluminando o meu caminho nos momentos mais difíceis. Ao Leonardo, meu filho, que consentiu as ausências prolongadas do pai durante este desafio.

palavras-chave Gestão de redes, monitorização, ferramentas

resumo

Os sistemas de gestão de rede alcançaram um papel de extrema importância em todas as áreas das tecnologias de informação e comunicação. À medida que as redes crescem em extensão, inovação tecnológica e heterogeneidade, todo o processo de gestão se torna mais complexo e exigente, e consequentemente, a implementação de sistemas de gestão torna-se crucial na detecção e prevenção de falhas; documentação, gestão e actualização das configurações de rede e de equipamentos; monitorização da utilização da rede para a contabilização do consumo de recursos; monitorização de desempenho para garantir a fiabilidade e alta qualidade de serviço; verificação dos acessos a recursos de forma a garantir o controlo e prevenção da utilização não autorizada. Este tipo de gestão não pode ser realizada somente pelo esforço humano, transversalmente pode investir-se na implementação de software específico, permitindo o ajustamento a características singulares da rede.

Esta dissertação apresenta um estudo de avaliação de ferramentas de gestão e monitorização de redes, enquadrando os princípios das áreas funcionais da gestão de redes, requisitos técnicos e funcionalidades. As ferramentas analisadas são baseadas em software livre e proprietário, e são direccionadas principalmente à gestão e monitorização de tráfego e dispositivos de rede. O ambiente escolhido para a implementação das plataformas foi primeiramente laboratorial tendo culminado na concretização de uma solução aplicacional em contexto real.

keywords **Network management, monitoring, tools**

abstract

Network management systems have reached an extremely important role in all information and communication technology areas. While networks grow in extension, technological innovation and heterogeneity, the management process becomes more complex and demanding, and consequently, the implementation of management systems becomes crucial in failure detection and prevention; documentation, management and update, of network and device configurations; network use monitoring to account for resource consumption; performance monitoring to ensure reliable and high quality network services; verification of access to resources to assure control and prevention of non-authorized use. This kind management cannot be performed only by human effort; transversally, it's possible to invest in implementing specific software, allowing for adjustment of specific network features.

This study presents an evaluation of network management and monitoring tools, contextualizing the principles of the functional areas of network management, technical requirements and functionalities. The analysed tools are open source and proprietary software, and are mainly directed towards the management and monitoring of network traffic and devices. The chosen environment for the implementation of the platforms was initially laboratorial, followed by the concretization of an applied solution in real context.

Índice

Índice de Figuras

Índice de Tabelas

1 Introdução

Os avanços tecnológicos têm hoje em dia um grande impacto na sociedade. A informação tem-se tornado, cada vez mais, uma vantagem competitiva para as empresas e organizações em investimentos futuros.

O facto é que, cada vez mais, as empresas, para se tornarem competitivas e sobreviverem no mercado, têm investido em tecnologia de informação, como a única forma de tornar seguro o processo de decisão. E é nesse quadro que as redes de computadores proliferam, encurtando as distâncias e diminuindo o tempo de resposta das transacções entre as organizações de todo o mundo.

1.1 Motivação

Em decorrência das vantagens que as redes de computadores oferecem, o número e a extensão destas estão em expansão continua. Assim, na medida que as redes crescem em escala e extensão, dois factores tornam-se mais evidentes: as redes, juntamente com seus recursos e aplicações, revelam-se cada vez mais indispensáveis para as organizações que as utilizam, logo, existe também uma maior possibilidade de ocorrerem problemas, o que pode levar as redes a um estado de inoperância ou a níveis inaceitáveis de desempenho.

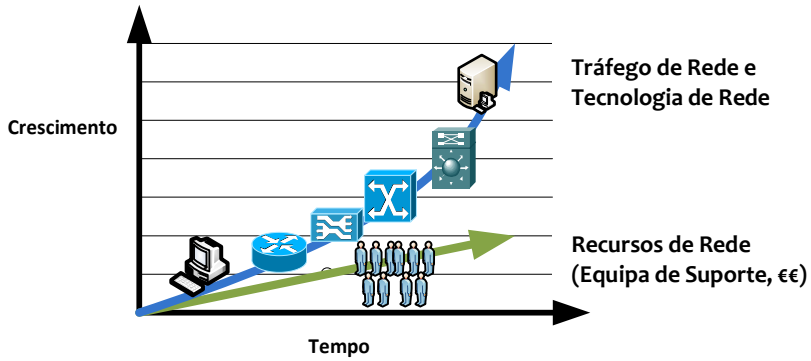


Figura 1 – Evolução do crescimento das redes

Assim, de forma a garantir a qualidade dos serviços aos seus utilizadores, as redes de computadores devem ser geridas. Esta gestão torna-se imprescindível, e envolve a monitorização e o controle de recursos distribuídos em redes. Na sua essência, a gestão de redes procura assegurar que sistemas de informação, disponíveis em redes, estejam operacionais e sejam eficazes.

Inicialmente, a de área de gestão de redes foi impulsionada pela necessidade de monitorização e controlo de dispositivos que compõem as redes de comunicação. Actualmente, a crescente complexidade das redes de dados, requer a utilização de ferramentas versáteis e de alto desempenho, na gestão, monitorização e análise de tráfego. Os dados fornecidos por estas ferramentas são fundamentais para a moderna gestão de redes, no dimensionamento e avaliação de redes.

Face à problemática exposta, esta dissertação apresenta um estudo de mercado de ferramentas de monitorização e gestão de redes, assim como um estudo de requisitos técnicos e funcionalidades. O trabalho realizado culmina na apresentação da solução aplicacional, para os sistemas de monitorização implementados no evento “Operação Pega-Monstro”, organizado pelo PmatE.

1.2 Estrutura

Esta dissertação encontra-se organizada em seis capítulos, estando estruturada de forma simples, apresentando registos que vão demonstrando o trabalho desenvolvido.

No primeiro capítulo é feita uma introdução, incluindo uma descrição global do trabalho desenvolvido, através de uma abordagem geral sobre a problemática e o enquadramento teórico realizado, reportando a estrutura da dissertação apresentada.

No capítulo dois, referente ao estado e enquadramento da arte, é abordada a temática da gestão de redes, fazendo a contextualização e a fundamentação teórica necessária à compreensão e conhecimento sobre o trabalho de investigação realizado. Neste capítulo são abordados temas de relevo para o enquadramento teórico, como por exemplo, modelos de gestão de redes, fazendo a referência e análise de protocolos disponíveis para o efeito.

O terceiro capítulo, refere-se à descrição das ferramentas de gestão e monitorização de redes analisadas, apresentando as suas funcionalidades e requisitos técnicos. Este capítulo é muito importante para a percepção das potencialidades das ferramentas.

O capítulo quatro apresenta a implementação das ferramentas, em ambiente laboratorial. Este é um capítulo fulcral para a compreensão dos processos de implementação das aplicações e sistemas envolvidos.

O capítulo cinco é um caso de estudo, e descreve a solução aplicacional (sistemas de monitorização) implementada no evento “Operação Pega-monstro”, realizado na Universidade de Aveiro.

O sexto e último capítulo desta dissertação, refere-se às principais conclusões obtidas através do desenvolvimento deste trabalho de investigação, apresentando as considerações finais, bem como, sugestões adequadas a soluções aplicacionais.

1.3 Terminologia

OSI - Open Systems Interconnection

RMON – Remote monitoring MIB2 extension

LMS – Lan Management Solution

TMN - Telecommunications Management Network

FCAPS – Fault, Configuration, Accounting, Performance, Security

ITIL - Information Technology Infrastructure Library

TI – Tecnologias de informação

NMS – Network Management System

DNS – Domain name system

IP - Internet Protocol

HTML - HyperText Markup Language

PERL - Practical Extraction and Report Language

SNMP - Simple Network Management Protocol

OID - Object Identifier

UPD - User Datagram Protocol

TCP - Transmission Control Protocol

NTOP - Network Traffic Probe

PHP - Hypertext PreProcessor

SMTP - Simple Mail Transfer Protocol

HTTP - HyperText Transport Protocol

ICMP - Internet Control Message Protocol

IETF - Internet Engineering Task Force

RFC - Request for Comments

MIB - Management Information Base

CDP – Cisco Discovery Protocol

SLA – Service Level Agreement

RRD – Round Robin Database

RRA – Round Robin Archive

CGI – Common Gateway Interface

CWLMS – CiscoWorks Lan Management Solution

CS – Common Services (CWLMS)

DCR – Device and Credential Repository (CWLMS)

CWA – CiscoWorks Assistant (CWLMS)

CM – Campus Manager (CWLMS)

RME – Resource Manager Essentials (CWLMS)

IPM – Internetwork Performance Monitor (CWLMS)

DFM – Device Fault Manager (CWLMS)

HUM – Health and Utilization Monitor (CWLMS)

CLI – Command line interface

2 Enquadramento

2.1 Introdução

Aproximadamente à duas décadas atrás, o clássico paradigma do agente-gestor centralizado foi a mais difundida arquitectura de gestão de rede, exemplificada no modelo de referencia OSI [1] e nas estruturas de gestão SNMP [3][4][5] e TMN [7]. Com o crescimento das redes (em expansão, complexidade de gestão e multiplicidade de serviços requeridos), aliado à importância que as mesmas têm assumido dentro das organizações, é exigida uma administração mais ampla e complexa. Consequentemente as redes assumem uma importância estratégica para as organizações, pois, uma falha na rede implicará um impacto directo no desempenho de uma organização. Para tal, os sistemas internos de gestão e monitorização vão permitindo aos administradores de redes e sistemas, saber instantaneamente se esses recursos estão operacionais ou não.

Actualmente, a administração de redes não considera apenas a monitorização de elementos de rede e outros equipamentos, mas também de serviços e aplicações. Com o crescimento da Internet, as redes de computadores tornaram-se maiores e mais complexas, exigindo ferramentas mais poderosas para monitorização e análise de ocorrências.

A gestão estratégica de todos os serviços e elementos das TI, é a chave para que os utilizadores usufruam de uma robusta infra-estrutura, permitindo às organizações gerir proactivamente a disponibilidade, utilização e crescimento dos serviços existentes na rede. A gestão proactiva possibilita a redução de indisponibilidade, redução de custos, e maior fiabilidade dos serviços.

A gestão de redes pode ser definida como [8]: todas as medidas que asseguram as operações efectivas e eficientes dos recursos de um sistema, em conformidade com os objectivos da organização. Para atingir o exposto, a gestão de redes é efectivada com o controlo dos recursos, gestão de serviços, monitorização, produção de alertas e relatórios relativos a anomalias e estado da rede.

Os objectivos da gestão de redes, podem ser definidos por:

- ✓ **Gerir os serviços e recursos da rede**: envolve o controlo, monitorização, actualização, e cadastro dos estados da rede; configuração de equipamentos e serviços existentes na rede.
- ✓ **Simplificar a complexidade da gestão da rede**: capacidade de um sistema de gestão de redes (NMS) disponibilizar a informação gerada, de uma forma compreensível. Um NMS também deverá estar habilitado para interpretar objectivos de gestão de alto nível.
- ✓ **Fiabilizar serviços**: fornecer alta qualidade de serviço, reduzindo a indisponibilidade. Os NMS deverão detectar e resolver erros e falhas na rede, e, disponibilizar segurança contra todas as ameaças que comprometem a segurança.
- ✓ **Consciencialização de custos**: Inventariação dos recursos e utilizadores da rede; monitorização e registo da utilização dos serviços existentes na rede.

Actualmente, à medida que as redes continuam crescer, mais dispositivos necessitam de ser geridos eficientemente, exigindo a melhoria constante de escalabilidade, no design da gestão de redes. Consequentemente, de forma a ser possível atingir os objectivos implícitos à gestão de redes, as directivas humanas apenas poderão ser entregues a um alto nível de abstracção e generalização.

2.2 Modelos de gestão de redes

Atingir compreensão e o domínio da gestão de redes pode alcançar-se através da adopção de modelos baseados em níveis superiores de abstracção. Existem duas estruturas: FCAPS e ITIL, que, embora não sejam soluções que abrangem a totalidade das circunstâncias, facilitam a decisão de tarefas de gestão e a avaliação de ferramentas de gestão de redes.

2.2.1 Modelo FCAPS

De a forma a atingir uma gestão focalizada, a ISO definiu, a partir do modelo OSI, cinco áreas funcionais: o modelo FCAPS, introduzido pelo ITU-T em Abril de 1997 na recomendação M.3400 [2].

A funcionalidade geral de gestão é então dividida em cinco áreas chave: gestão de falhas (Fault management), gestão de configurações (Configuration management), gestão de contabilidade (Accounting management), gestão de desempenho (Performance management) e gestão de segurança (Security managment). Esta categorização é funcional, e não descreve assuntos relacionados com negócio, de um sistema de gestão numa rede de telecomunicações. O FCAPS é directamente alicerçado pelas recomendações do ITU-T, e descreve os cinco tipos de informação manipulada pelos sistemas de gestão.

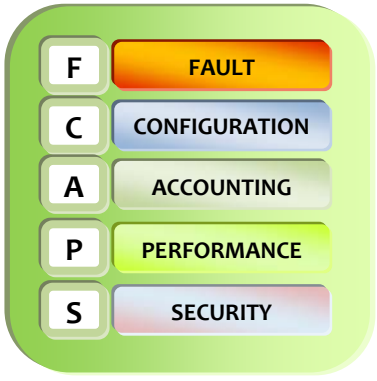


Figura 2 – Modelo FCAPS

2.2.1.1 Gestão de Falhas

Reconhecer situações problemáticas é a primeira demanda da *gestão de falhas,* como a detecção da inesperada inoperância de um sistema, dispositivo ou componente de rede. As falhas são identificadas por erros excessivos, como erros de alinhamento *Ethernet.* Porém, nem todos os erros são considerados como falhas, alguns, como as colisões num ambiente Ethernet, são normais, desde que não excedam um limiar aceitável. Um eficaz sistema de gestão de falhas, também deverá ser capaz de isolar os problemas na fonte, providenciar notificações para a(s) pessoa(s) apropriada(s) e solucionar as ocorrências através de um sistema de *Ticketing.* A gestão de falhas é então definida por: detecção, isolamento e correcção de falhas persistentes ou transitórias, que possam causar o colapso da rede de forma inesperada.

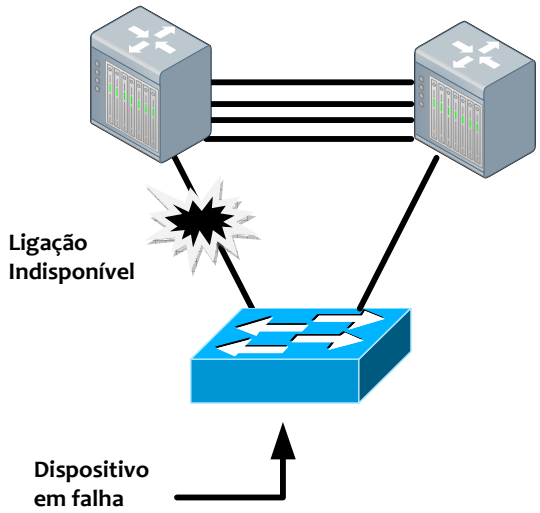


Figura 3 – FCAPS - Falha na estrutura física da rede

A monitorização é a base dos sistemas de gestão de falhas, na qual está incluída a recolha de informações referentes a *hardware* e *software* dos equipamentos; também poderá incluir a recolha de dados acerca do estado, robustez e desempenho dos dispositivos. Sinteticamente, a monitorização envolve a análise e a produção de relatórios acerca dos dados recolhidos.

2.2.1.2 Gestão de Configurações

A essência de todas as tarefas de gestão de redes é documentar e entender a rede. É essencial atingir uma clara noção da conectividade e sua configuração, para assegurar uma manutenção efectiva e a resolução de problemas à medida que estes surgem.

A gestão de configurações alicerça a área fundamental que gere a configuração dos equipamentos. É uma das mais importantes formas que um administrador de rede dispõe para controlar a estabilidade da rede, mantendo um regular agendamento de cópias de segurança e um controlo metódico das implementações e procedimentos de alteração que possam ser alcançados. Outro aspecto a considerar, refere-se à capacidade de registo e monitorização das alterações que são efectuadas na configuração dos equipamentos. Manter com precisão um arquivo de todas as configurações, é a chave para o controlo efectivo dos dispositivos, devido à possibilidade de aceder em tempo útil à informação vital das suas configurações, permitindo proceder a comparações e alterações à medida que forem necessárias. É relevante salientar também, a importância de manter seguro e preciso o sistema de monitorização e registo, que armazena os ficheiros de configuração que são implementados na rede.

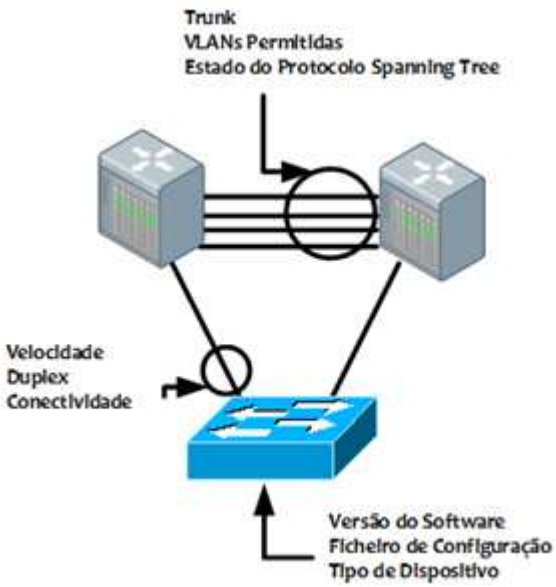


Figura 4 – FCAPS – Gestão de configurações

2.2.1.3 Gestão de Contabilidade

A gestão de contabilidade centra-se em estatísticas de utilização e alocação de custos, associados a encargos ao longo do tempo e serviços disponibilizados pelos dispositivos e recursos da rede. Os sistemas de gestão de contabilidade focam-se na forma como os recursos da rede são utilizados, mas em vez de olhar a utilização de recursos sob um ponto de vista do desempenho da rede, este tipo de gestão preocupa-se em saber, por quem os recursos são utilizados, quais os utilizadores que consomem mais recursos, quais os sistemas ou aplicações que consomem maior largura de banda, etc. Os resultados provenientes destas tarefas, fornecem às organizações a capacidade de crescimento direccionado à utilização desses recursos, e, por conseguinte, assistem os administradores de rede a planear com precisão um crescimento antecipado.

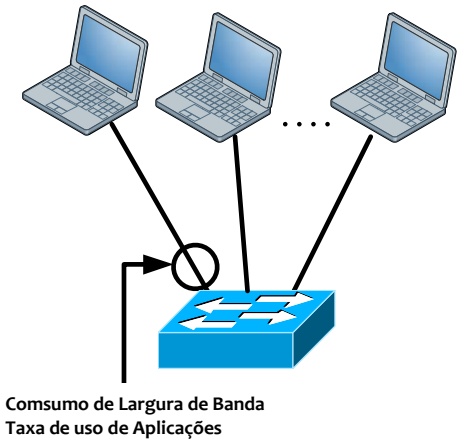


Figura 5 –FCAPS - Contabilização do consumo de recursos

2.2.1.4 Gestão de Desempenho

O objectivo da gestão de desempenho assenta na monitorização, avaliação e produção de alertas, do comportamento e eficiência da estrutura lógica e física da rede, incluindo dispositivos, ligações, circuitos, sistemas e aplicações. A informação gerada por este tipo de gestão, apresenta um papel importante, quer na monitorização em tempo real, quer para fins de histórico de alertas. Por exemplo, os sistemas de gestão de desempenho, podem ser usados para recolher informação de dispositivos de rede, ligações, sistemas, componentes ou aplicações, em tempo real, para alertar as organizações de suporte acerca de problemas de desempenho, assim como, armazenar a recolha desses dados ao longo do tempo, para identificar padrões de utilização, tais como os fluxos de dados em ciclos de uma hora, semanais, mensais…; A informação de desempenho também pode ser usada para identificar tendências, proporcionando uma maior capacidade de planeamento para a rede e actualização de sistemas.

A gestão de desempenho, vê a rede como um todo, em todas as ligações ponto a ponto, identificando estrangulamentos no desempenho e disponibilizando informação para encontrar soluções para problemas. Foca-se em métricas de avaliação, que indicam como os recursos da rede são utilizados, o desempenho dessa utilização, e como estes padrões de uso afectam a entrega dos serviços de rede, para análise corrente e planeamento futuro.

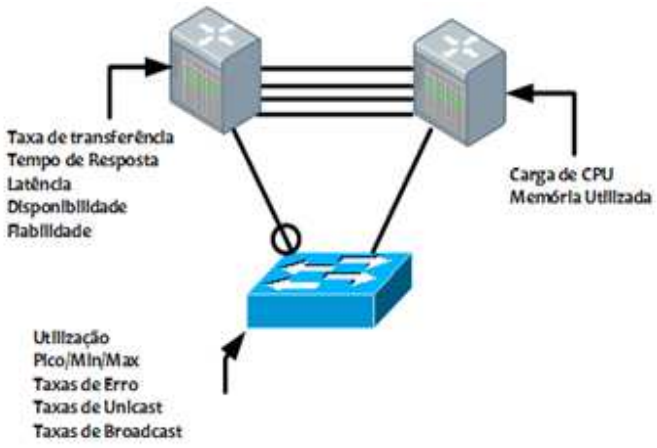


Figura 6 – FCAPS - Identificação de variáveis de desempenho

2.2.1.5 Gestão de Segurança

O objectivo primordial da gestão de segurança é protecção contra o acesso não autorizado, a redes, sistemas e dados. Representa uma preocupação relevante para as equipas técnicas e de gestão, pelo facto de a segurança da rede se estender para além da própria rede. Estende-se para o ambiente físico, que também controla o acesso a redes e dados. Portanto, a gestão de segurança, deve incluir a definição de políticas por parte das equipas envolvidas, para assegurar o acesso seguro a redes, envolvendo o acesso seguro e a manipulação segura de dados que residem na rede. Também deverá incluir a identificação de procedimentos a seguir, quando um problema de segurança ocorre.

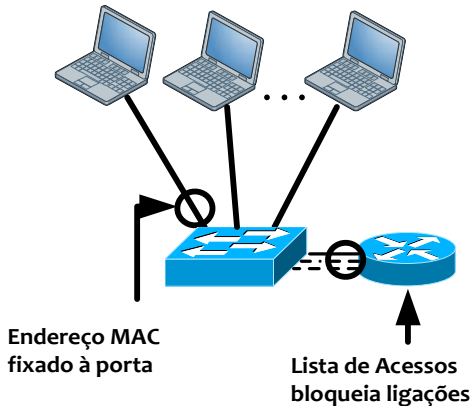


Figura 7 – FCAPS - Aplicação de medidas de segurança

Resumindo, a gestão de segurança pretende fornecer protecção contra todas as ameaças de segurança a recursos, serviços e dados na rede, e, em adição, garantir a privacidade aos utilizadores e controlar as permissões de acesso.

2.2.1.6 Sub-funcionalidades do FCAPS

O quadro seguinte apresenta um conjunto de sub-funcionalidades do modelo FCAPS para uma das suas áreas.

F	C	A	P	S
Detecção de Falhas	Inicialização de recursos	Serviço de rastreio / Utilização de recursos	Utilização e taxas de erros	Acesso selectivo a recursos
Correcção de falhas	Aprovisionamento de recursos	custo dos serviços	Nível de desempenho consistente	Activar Funções dos elementos de rede
Isolamento de falhas	Auto-descoberta	Limites contabilisticos	Colecção de informação de desempenho	Acesso a logs
Restauração da rede	Cópias de segurança e restauro	Relacionar custos de múltiplos recursos	Produção de relatórios de desempenho	Alertas de segurança / relatórios de eventos
Tratamento de alertas	desactivação de recursos	Definição de cotas	Análise da informação de desempenho	Privacidade de dados
Filtragem de alertas	Gestão de alterações	Auditorias	Relatórios de problemas	Verivicação de permissões de acesso
Produção de alertas	Pre-provisionamento	Relatorios de Fraudes	Planeamentos de competências	Resuloção de quebras de segurança
Correlação de remoções	Gestão de activos /inventário	Suporte para direrentes modos de contabilidade	Informação de desempenho e colecção de estatisticas	Security audit trail log
testes diagnóstico	Cópia de configurações		Manutenção e análise de Historiais	Distribuição de informações relacionadas com segurança
Relatórios de erros	Configuração remota			
Tratamento de erros	Inicialização, rastreio e exewcução de tarefas			
Estatisticas de erros	Distribuição automatizadade software			

Tabela 1 – Sub-funcionalidades do FCAPS

2.2.2 Modelo ITIL

O modelo ITIL [9] (Information Technology Infrastructure Library) representa um conjunto de regras de boas práticas para a gestão de Tecnologias de Informação. Foi criado pela CCTA (United Kingdom's Central Computer and Telecommunications) no final dos anos 80, para dar resposta à crescente dependência em TI sentida pelas organizações, indo ao encontro das necessidades e objectivos de negócio. Acompanhando a evolução do mercado e das novas tecnologias, o ITIL sofreu revisões, das quais duas se destacam: a que deu origem à versão dois, já sob a alçada da OGC (Office for Government of Commerce) no ano 2000, e a que deu origem à versão três (ITIL V3) em 2007.

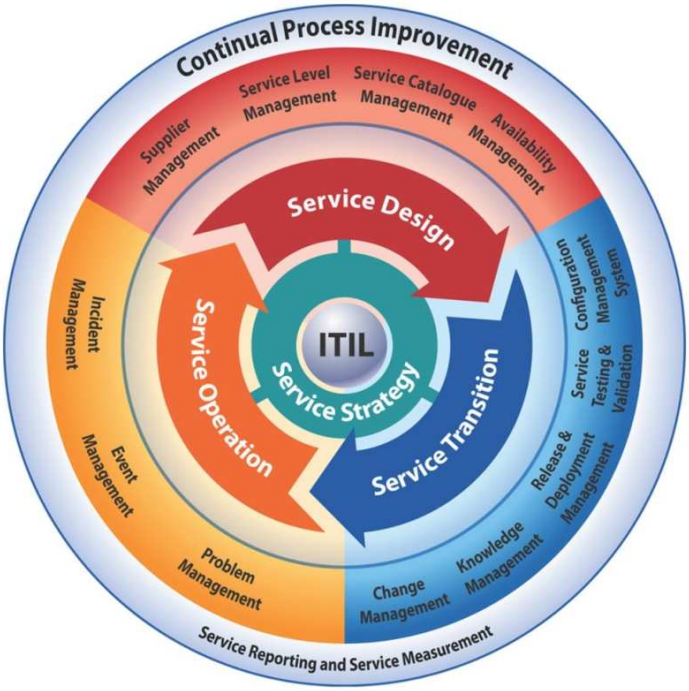


Figura 8 – Estrutura do modelo ITIL v3

O ITIL foi desenhado para garantir qualidade de serviço e consequentemente melhorar as práticas de gestão de redes. Estas práticas incluem estruturas de administração de equipamentos, aplicações, serviços e segurança. Para cada uma dessas áreas são designados processos relativos aos estados do ciclo de vida da gestão de serviço.

O ciclo de vida da gestão de serviço no ITIL V3 é constituído pelos seguintes estados (Figura 8):

- Service Strategy (Estratégia de serviço)
- Service Design (Design de serviço)
- Service Transition (Transição de serviço)
- Service Operation (Operação de serviço)
- Continuous Service Improvement (Melhoria contínua de serviço)

Para além de um conjunto de normas e boas práticas, o ITIL V3 fornece uma estrutura que facilita a avaliação de ferramentas de gestão de redes, em que se destacam os seguintes processos:

- ***Incident Management*** *(Gestão de Incidentes)**:*** O objectivo deste processo é a verificação e análise de incidentes, visando a máxima expansão da disponibilidade dos serviços. Na ocorrência de incidentes, os serviços deverão ser restabelecidos o mais rápido possível, para minimizar impactos adversos nas operações de uma organização. Segundo o ITIL v3, cada incidente gera um problema.

- ***Problem Management*** *(Gestão de Problemas)**:*** Tem o objectivo de fornecer a prevenção proactiva da ocorrência de incidentes, problemas e erros numa infra-estrutura de TI, de forma a reduzir o impacto destas ocorrências.

- ***Configuration Management*** *(Gestão de Configurações)***:** obriga à padronização de sistemas e métodos, de forma que a implementação, detecção e correcção de problemas ocorra da forma mais simples e linear possível. Tem como objectivo principal fornecer um modelo lógico da infra-estrutura de TI pela identificação, manutenção e verificação das versões de todas as configurações existentes. Mais do que um simples registo dos activos físicos, inclui documentação, acordos a nível de serviço, catálogos de serviço, garantias e conhecimento. Outro aspecto a salientar é a imposição de uma base de dados de gestão de

configurações (CMDB - Configuration Management Database) que se traduz como um repositório de informação acerca dos activos e serviços de TI de uma organização, e a relação entre estes. A CMDB fornece uma fonte única de informação que pode ser referenciada e partilhada pelos outros processos de gestão de serviço. Deste modo a qualidade da informação armazenada na CMDB afecta a eficiência de toda a estratégia do ITIL. A informação relativa a configurações, fornece um meio para melhorar o desempenho, através da adaptação e antecipação de alterações necessárias, mantendo assegurada a disponibilidade e segurança das infra-estruturas de TI.

- ***Change Management*** *(Gestão de Alterações)***:** As alterações em serviços poderão ter um impacto negativo nos processos de uma empresa, pois novos hábitos, novas rotinas e novas tarefas representam um constrangimento no processo produtivo, mesmo que o seu objectivo seja facilitar esse mesmo processo. As alterações deverão ocorrer mantendo a mesma qualidade dos serviços. O objectivo global do *Change Management* é assegurar a utilização de métodos e procedimentos estandardizados para a manipulação de todas as alterações, de forma a minimizar o impacto de quaisquer incidentes relacionados.

- ***Release Management*** *(Gestão de Implementações)**:*** O objectivo deste processo é facilitar a introdução de novo software e hardware nos ambientes de TI. Mais do que alterações tecnológicas, muitas vezes a equipas de TI terão de lidar com o impacto psicológico provocado por novas implementações. Deste modo pretende minimizar impactos negativos numa organização causados por alterações que são introduzidas, e está intimamente integrado com os processos *Change Managment* e *Configuration Managment* de forma a assegurar que quaisquer alterações necessárias na infra-estrutura de TI, são implementadas de uma forma segura e eficiente.

- **Availality Managment** (Gestão de Disponibilidade)**:** A este processo cabe a tarefa de optimizar a capacidade de uma infra-estrutura de TI e organização de apoio, para fornecer disponibilidade a um custo eficaz e a nível sustentado, que permita a satisfação dos objectivos acordados.

- **Service Level Managent** (Gestão a nível de serviço): O objectivo deste processo é fornecer uma gradual melhoria da qualidade de serviço, através de um ciclo constante de estabelecimento de acordos, monitorização, notificação, e revisão dos objectivos de serviço, e por instigar acções para erradicar níveis de serviço inaceitáveis. Este processo qualifica e quantifica as expectativas do cliente e a capacidade das TI na entrega dessas expectativas. O resultado deste balanceamento é formalizado num acordo de nível de serviço (SLA – Service Level Agreement)

2.3 Protocolos de gestão e monitorização

2.3.1 Técnicas de monitorização

Presentemente, existem dois tipos de técnicas de monitorização: a activa (intrusiva) e a passiva (não intrusiva).

A técnica de monitorização activa consiste na injecção de pacotes de controlo na rede. Esses pacotes atravessam todo o caminho da rede a ser medido e são recolhidos num ponto. Através das informações recolhidas, algumas medidas de desempenho podem ser extraídas. Dependendo da informação a ser extraída, os pacotes devem transportar dados que serão analisados no receptor.

A chamada de monitorização passiva, apenas observa os pacotes que passam pela rede. Ao contrário da monitorização activa, as técnicas passivas não injectam pacotes. Desta forma, monitores, que funcionam em modo promíscuo, são colocados no caminho dos pacotes para recolher informações que, posteriormente, serão analisadas. Apesar de não sobrecarregar a rede com pacotes adicionais, equipamentos e softwares sofisticados podem ser necessários para fazer a recolha e a análise dos dados.

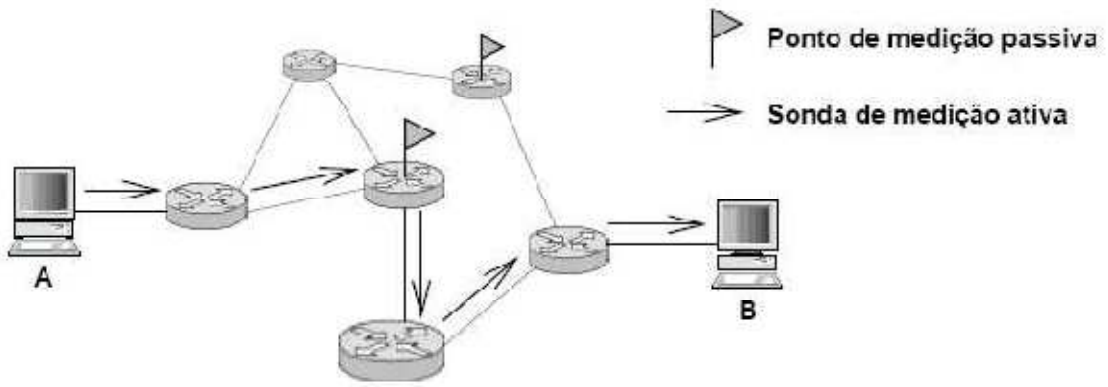


Figura 9 – Exemplo de monitorização activa e passiva

2.3.2 SNMP

O SNMP [3] (Simple Network Management Protocol) é um protocolo ao nível da aplicação que facilita a troca de informações entre as estações de gestão e os agentes residentes nos elementos geridos, como routers, switches, servidores, entre outros. Uma rede gerida por SNMP possui três elementos chave: os dispositivos geridos, os agentes e as estações de gestão. Através desta infra-estrutura, o SNMP disponibiliza aos administradores de rede informações sobre a utilização dos recursos e alarmes, o que permite identificar e solucionar problemas, e planear o crescimento da rede. Os dispositivos geridos, recolhem e armazenam as informações na sua base de dados (Management Information Base - MIB) e disponibilizam-na, via SNMP, para as estações de gestão. O agente tem função específica de recolher os dados armazenados na MIB e transformá-los em informações compatíveis com SNMP.

O padrão MIB que contempla a base de dados relacionado com dados referentes a de tráfego é a MIB-II (Figura 10). A sua organização contém um conjunto de grupos que monitorizam a execução de vários protocolos no elemento de rede, como o IP, TCP/UDP, BGP, OSPF, fornecendo o estado (activo/inactivo) das interfaces de um equipamento ou contabilizando as estatísticas dos contadores de bytes e pacotes enviados, recebidos ou perdidos para cada interface. Disponibilizam ainda, informações sobre dados relevantes relativos ao desempenho do dispositivo, como utilização de CPU e memória.

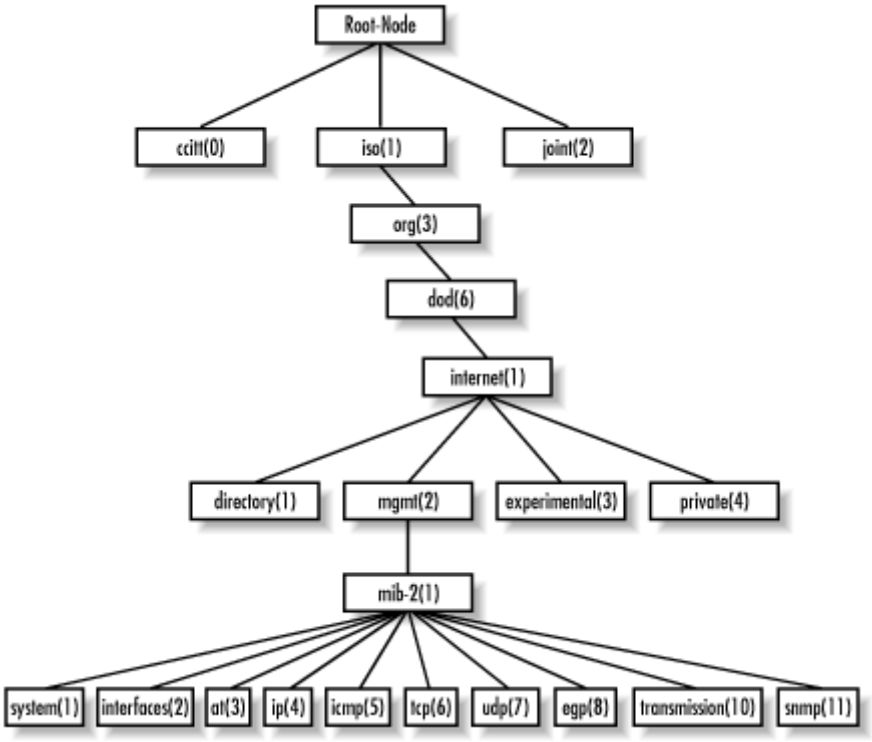


Figura 10 – MIB II

2.3.3 RMON

O RMON [3], é uma extensão da MIB II que define um conjunto de estatísticas e funções que podem ser trocadas via SNMP, entre várias probes e gestores estabelecidos em toda a rede. O RMON possibilita vantagens já que permite obter informação sobre os segmentos ethernet como um todo e não apenas do *host* como acontece na MIBII. O RMON I apenas dá estatísticas até ao nível MAC. Já o mais recente RMON II, dá estatísticas a nível de aplicação. Existem 9 grupos RMON (statistics, history, alarm, host, hostTopN, matrix, Filter, packet capture e event) sendo que cada um destes grupos dá informação que vai de encontro a necessidades de monitorização de redes.

2.4 Conclusões

Enquanto o FCAPS é um excelente modelo para definir os objectivos da gestão de redes de uma forma funcional, o ITIL apresenta uma aproximação de boas práticas na entrega de serviços, alinhando-se com as actuais estruturas organizacionais das TI, expandindo a abrangência do modelo FCAPS.

No âmbito desta dissertação, o enquadramento dos modelos de gestão expostos, terá maior incidência no modelo FCAPS, devido às características funcionais que apresenta.

As técnicas de monitorização abordadas podem ser inseridas simultaneamente na gestão de uma rede, pois podem representar diferentes papeis adatpados a necessidades especificas de gestão. As ferramentas analisadas nos seguintes capitulos, utilizam as técnicas de monitorização activa e passiva e são ,maioritáriamente, baseadas na arquitectura SNMP. Também será estudada uma ferramenta de monitorização passiva baseada em *Libpcap*.

3 Ferramentas de Gestão e Monitorização

3.1 Introdução

Tradicionalmente, as ferramentas de gestão de redes são separadas em linhas distintas de operação: gestores de elementos de um específico fabricante, plataformas de gestão de redes focalizadas primordialmente na gestão de falhas e eventos, e soluções de gestão de desempenho.

Nenhuma ferramenta de gestão de elementos em redes contém funcionalidades para gerir com eficiência todos os tipos de dispositivos de rede. Tipicamente, os fabricantes de equipamentos de rede, não vão despender recursos críticos, para desenvolver ferramentas direccionadas à gestão de equipamentos de outros fabricantes. Por esta razão, ferramentas de gestão de elementos desenvolvidos por um específico fabricante, são as que melhor se adequam à gestão dos detalhes particulares dos seus equipamentos.

Os "NMSs" (como por exemplo o HP Open View) são a melhor solução para a gestão total da infra-estrutura da rede (Figura 11) nos termos de disponibilidade e notificação de eventos.

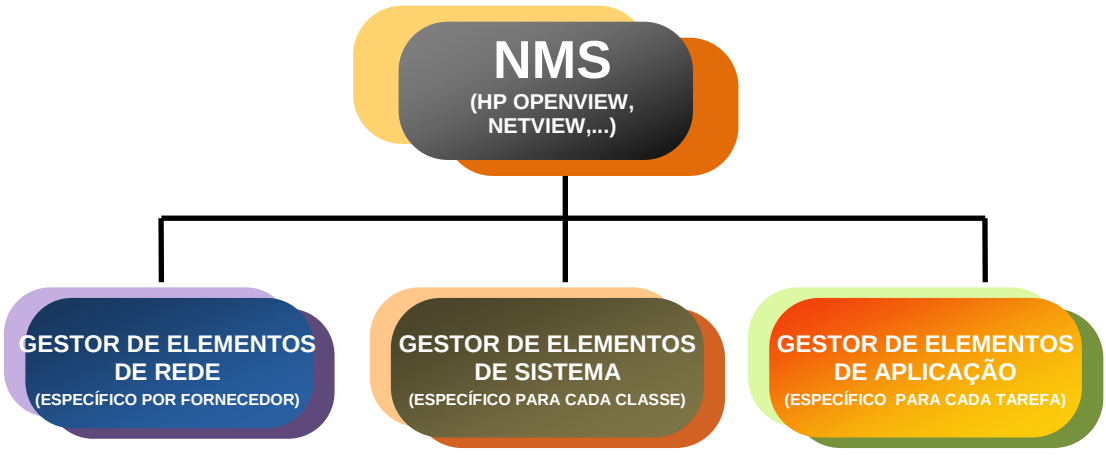


Figura 11 – Componentes de uma infra-estrutura de gestão de rede

As ferramentas de gestão de elementos (Figura 11) podem ser classificadas nas três seguintes categorias básicas:

- Gestores de elementos de rede: Tipicamente direccionados à gestão de uma ou mais áreas funcionais da gestão de rede, de equipamentos de um especifico fabricante.
- Gestores de elementos de sistema: gerem uma classe de elementos, de um ou mais fabricantes, como por exemplo, sistemas operativos e dispositivos.
- Gestores de elementos aplicacionais: gestão orientada à tarefa, como por exemplo: DHCP, DNS, ou telefonia IP.

As ferramentas abordadas neste trabalho, abrangem no seu conjunto todas as áreas funcionais da gestão de redes, e são direccionadas à gestão e monitorização de redes e seus elementos, e monitorização de tráfego:

- **CiscoWorks LMS**: gestão e monitorização de equipamentos Cisco.
- **Cacti**: monitorização de tráfego e elementos de rede
- **Nagios**: monitorização da disponibilidade de dispositivos e serviços
- **NTOP**: monitorização passiva de tráfego

3.2 Cacti

Cacti [10] é uma solução completa para apresentação de gráficos de rede, desenhada para tirar proveito das potencialidades da ferramenta RRD Tool no armazenamento de dados e disponibilização dos mesmos graficamente.

Das diversas funcionalidades do Cacti destacam-se as seguintes características: contém um "poller de alto desempenho, avançadas características dos modelos para criação de gráficos, múltiplos métodos para aquisição de dados, funcionalidades para gestão de acesso a utilizadores. Todas estas características convergem numa intuitiva interface (Figura 12) de utilização simples, adaptável à gestão de redes de pequena dimensão até redes complexas que contêm centenas de equipamentos.

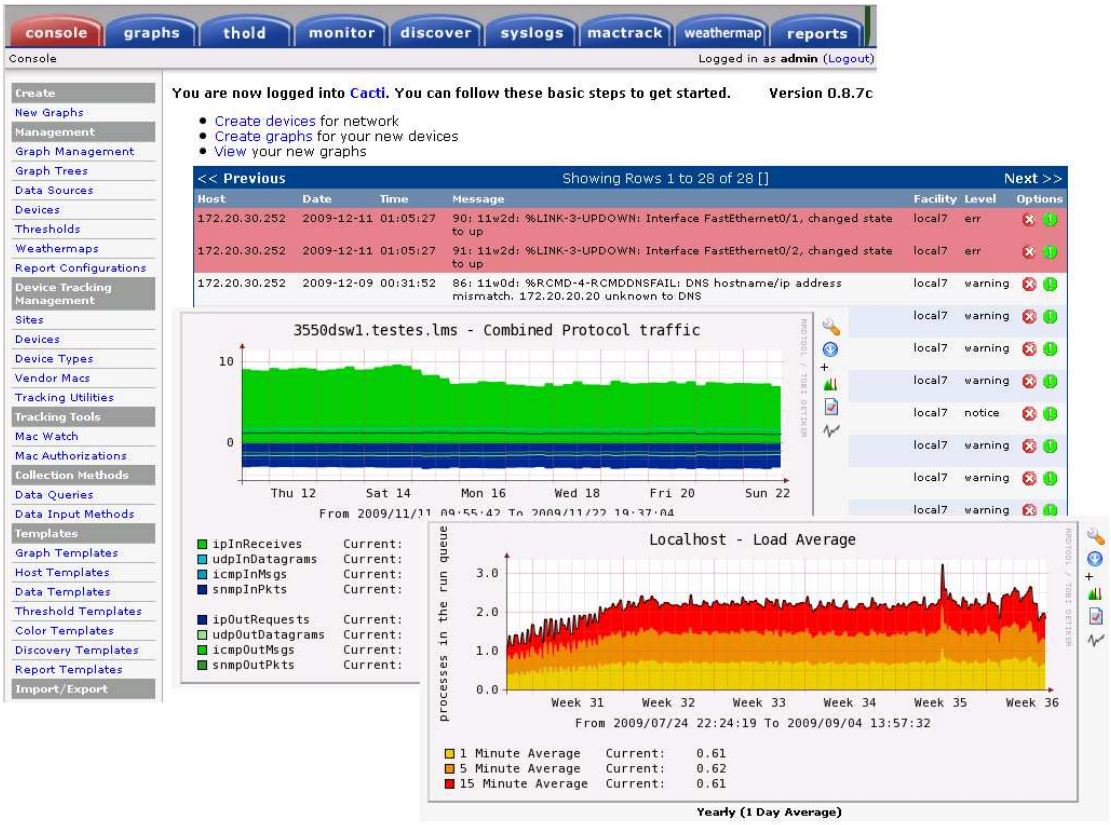


Figura 12 – Interface Web do Cacti

RRD Tool [13] é um programa em C escrito por Tobi Oetiker, autor do conceituado MRTG – Multi Router Traffic Grapher, sendo considerado como a geração seguinte deste. O RRD Tool inclui uma completa "re-implementação" das características de grafismo e de registo do MRTG.

RRD é a sigla de "Round Robin Database". É um tipo de base de dados desenhado para armazenar sequências de informação obtidas num determinado período de tempo (largura de banda da rede, temperatura de uma máquina, etc), sem aumentar de tamanho. Em termos de computação, este tipo de estrutura de dados, em que o ultimo valor é eliminado cada vez que um novo é adicionado, é um *"ring buffer".* Estes *"Ring Buffers"* são chamados *"round-robin archives"* ou RRAs e armazenam uma taxa.

O RRD Tool é uma ferramenta de manipulação de RRDs e é capaz de gerar gráficos a partir da informação recolhida, mas como não é capaz de fazer o *"polling"* dos dados, nem apresenta-los de forma automática, é comum a sua utilização ser associada a um *"front-end"*. O Cacti é um "*front-end"* para o RRDTool escrito em PHP. Com esta ferramenta é possível fazer o *"polling"* constante de *"hosts"* SNMP, criar gráficos a partir da informação obtida, e gerir o acesso de utilizadores à visualização dos resultados. Pode substituir com vantagens a ferramenta MRTG, frequentemente utilizada para a criação de gráficos de utilização de largura de banda. O Cacti utiliza um conjunto de aplicações para realizar a visualização gráfica de resultados obtidos via SNMP, estes valores podem ser taxas de entrada/saída de uma rede, número de endereços MAC associados a um *acess-point*, etc.

O recurso à utilização de SNMP para gerir uma rede pode possibilitar um ponto central de consolidação e monitorização saudável de uma infra-estrutura, visto estar presente e poder ser facilmente activado em muitos dispositivos de rede. A utilização de SNMP para constantemente obter informação estatística e apresenta-la em gráficos, tem a utilidade de poder disponibilizar o acompanhamento de variadas características existentes numa infra-estrutura tais como: utilização de disco, actividade na rede, etc.

O princípio de operação do Cacti [11] segue uma filosofia cliente-servidor e é constituído pela seguinte sequência de tarefas:

1. Recolha de dados: Esta tarefa é efectuada através da utilização do poller para a aquisição de informação (maioritariamente SNMP) dos dispositivos de rede, sendo a execução deste sincronizado pelo gestor de eventos do sistema operativo.
2. Armazenamento de dados: O Cacti utiliza a ferramenta RRDTool para guardar a informação proveniente do "polling" de dados em formato RRD. Esta informação é armazenada de um modo compacto que não se expande ao longo do tempo. Da mesma forma realiza a consolidação de dados, disponibilizando algumas funções como, por exemplo, médias, máximos, mínimos, e últimos valores observados.
3. Apresentação de dados: É efectuada através da combinação das potencialidades avançadas de grafismo da RRDTool com um Servidor Web, o que torna o acesso aos dados disponível a partir de qualquer browser Web.

Plug-in's

Em complemento às funcionalidades básicas do Cacti, existem diversos plugins oficiais [12][14], que oferecem utensílios de diagnóstico, notificação e aquisição de informação, assim como melhorias no desempenho do sistema de monitorização. Dos plugins mais utilizados comummente, são aqui destacados os seguintes:

- **Discovery**: Realiza a auto-descoberta de dispositivos não monitorizados pelo Cacti, em sub-redes especificadas. Os dispositivos descobertos são apresentados numa lista que fornece informações acerca do estado SNMP, e de conectividade de cada um, possibilitando a adição automatizada dos mesmos ao Cacti através de templates, e consequentemente a criação de gráficos baseados na descrição do sistema.

- **Flowviewer:** Gera relatórios baseados em informação gerada pelo protocolo Netflow (Cisco), relativa a fluxos tráfego.
- **Mac Track:** Examina os dispositivos de rede com o objectivo de localizar um dispositivo específico. É um plugin bastante interessante no campo da gestão de segurança, pela capacidade que fornece para encontrar fontes de propagação de vírus e localização de equipamento furtado. As funcionalidades relevantes são as seguintes:
    - Rastreio de dispositivos
    - Identificação de endereços Mac
    - Associação de endereços IP com endereços Mac
    - Inventariação de portos
    - Notificação acerca de dispositivos ligados não autorizados.
- **NTop:** Permite a visualização da aplicação NTOP, integrada no Cacti via iFrame.
- **Realtime:** Fornece um método de visualização de gráficos com uma resolução mínima de cinco segundos. Um plugin bastante interessante para a realização de diagnósticos em tempo real.
- **RouterConfigs:** É uma ferramenta que permite visualizar e armazenar cópias de seguança da configuração de roteadores Cisco, através de suporte telnet.
- **Syslog:** Permite a recepção, armazenamento numa base de dados e visualização de mensagens de syslog enviadas pelos dispositivos de rede. Adicionalmente permite também a configuração de alertas relativos a mensagens críticas, e a filtragem de mensagens a guardar.
- **Thold:** Fornece capacidade para a configuração de limiares aceitáveis relativos a valores atingidos nos gráficos, e a definição de notificações de alerta quando estes valores são ultrapassados e quando ocorrem falhas de conectividade nos dispositivos.
- **Monitor**: Adiciona um separador no interface Web do Cacti, que mostra objectos referentes ao estado de conectividade dos dispositivos. Permite a activação de alertas sonoros quando ocorrem falhas de conectividade.

- **Weathermap**: É uma ferramenta que permite a visualização de rede, utilizando informação existente para gerar mapas de fluxos de tráfego. A integração deste desta ferramenta no Cacti, permite a visualização dos mapas de rede através do seu sistema de controlo de acessos.

O Cacti é distribuído sob licença *GNU General Public License v2 (GPL),* pelo que não apresenta encargos de utilização e pode ser livremente adquirido online no sítio oficial (http://www.cacti.net/).

Requisitos de hardware e software

Esta aplicação é compatível com sistemas Microsoft Windows, Linux e a maioria das variantes Unix. Os requisitos mínimos de software, apresentados nos manuais fornecidos pela equipa de desenvolvimento (versão 0.8.7e), são os seguintes:

- RRDTool 1.0.49 ou 1.2.x
- MySQL 4.1.x or 5.x
- PHP 4.3.6 ou 5.x (versões actuais são recomendadas para funcionalidades avançadas)
- Servidor Web - Apache or IIS

Quanto aos requisitos mínimos de hardware, não existem menções nos manuais e documentação adicional. Pelo que se conclui que estes requisitos se prendem fundamentalmente aos requeridos pelo sistema operativo em que o Cacti irá ser instalado. Embora se comprove, através de experiência profissional e alguma pesquisa em fóruns de discussão [12], bom desempenho com poucos recursos de hardware (como por exemplo CPU PIII 1GHz e 512 MB RAM) em redes de pequena dimensão com algumas dezenas de dispositivos, a implementação em redes de média e grande envergadura com centenas de equipamentos requer um acréscimo de recursos em consonância com o número de dispositivos e gráficos pretendidos.

3.3 Nagios

Nagios [19] é uma aplicação *Open Source* concebida para a monitorização de dispositivos e serviços de rede, tendo como objectivo principal a gestão de disponibilidade. Embora inicialmente tenha sido projectado para monitorizar apenas aplicações e sistemas, o desenvolvimento de *plugins* em torno do seu processo central, tornou-a actualmente numa ferramenta amplamente utilizada para a monitorização de disponibilidade em redes. Esta aplicação foi desenhada para correr em sistemas operativos Linux, mas apresenta compatibilidade com a maioria das variantes Unix, tais como o FreeBSD, OpenBSD e NetBSD .

Como já foi referido, o seu funcionamento é suportado por um conjunto de plugins que providenciam informações acerca do estado de serviços locais e remotos, dos quais a eficácia de monitorização do Nagios numa rede, depende da expansão dos mesmos. O monitor de execução (*daemon*) do Nagios, realiza verificações periódicas nos dispositivos e serviços, especificados através de *plugins* externos que retornam a informação pretendida. Na ocorrência de incidentes, logo que são detectados, o Nagios encontra-se provido da capacidade de gerar notificações, e envia-las em diversos formatos, como por exemplo correio electrónico ou SMS, para os agentes envolvidos na administração da rede. A visualização do estado actual, histórico e relatórios, dos elementos monitorizados, é disponibilizada via interface Web.

A implementação desta aplicação é orientada a redes de grade dimensão, apesar de apresentar excelente desempenho em redes de pequeno porte. É uma solução de monitorização demonstrada quer pela capacidade de alertar a indisponibilidade de serviços e dispositivos de rede especificados nos ficheiros de configuração, quer pela capacidade de monitorizar equipamentos com suporte SNMP. A criação de *plugins* personalizados é uma tarefa acessível, recorrendo à concepção de scripts escritos em CGI (*Common Gateway Interface*), ou a outras linguagens de programação como C ou Pearl.

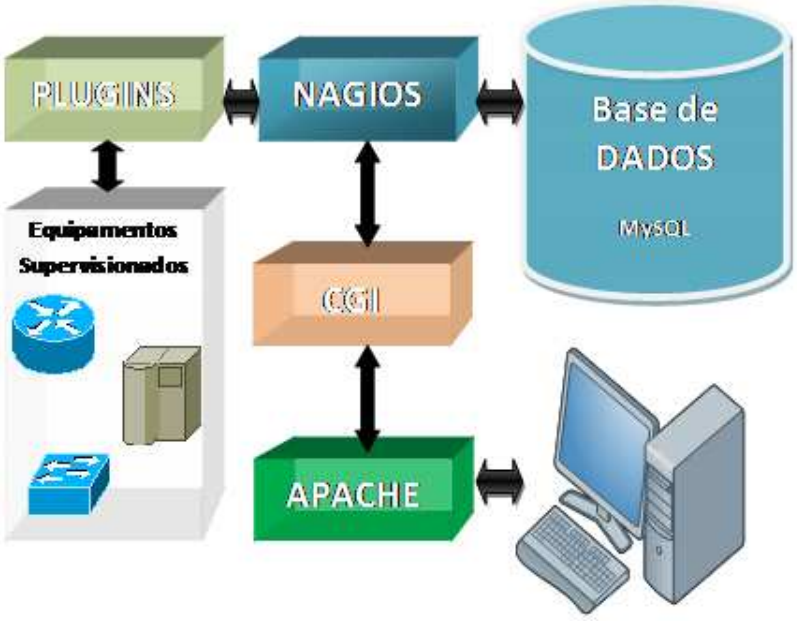


Figura 13 – Arquitectura do Nagios

As principais funcionalidades do Nagios são as seguintes:

- Monitorização de serviços de rede: POP3, SMTP, HTTP, Ping, NNTP, DNS, etc.

- Monitorização de recursos: carga de processador, utilização de disco e memória RAM, processos em execução, etc. Inclui sistemas Windows através da instalação de um agente nas máquinas clientes.

- Organização simples de *plugins* que permite aos administradores facilmente desenvolver os seus próprios serviços monitorização.

- Definição de hierarquia de *hosts*, admitindo a criação de grupos em que os dispositivos são agrupados em níveis de prioridade, permitindo a detecção e distinção entre os que estão inoperantes e aqueles que estão inalcançáveis

- Definição de manipuladores de eventos (*event handlers*) que serão executados durante ocorrências nos serviços ou dispositivos, com o intuito de resolução de problemas.

- Suporte para implementação de sistemas de monitorização redundantes.

- Notificação de contactos na ocorrência e resolução de problemas via correio electrónico, SMS, *Instant messages*, e outros métodos possíveis de definir pelos administradores.

- Interface Web para visualização do estado actual da rede, histórico de notificações e ocorrências, relatórios, etc.

- Integração com eSensor, para a monitorização de variáveis ambientais como temperatura, iluminação e humidade.

- Rotatividade automática dos arquivos de *logs*

Uma grande vantagem do Nagios é o facto de ser software livre, distribuído sob licença *copyleft GPL,* encontrando-se disponível para download no sítio Web www.nagios org, assim como um vasto leque de plugins oficiais.

Requisitos de hardware e software

Os únicos requisitos para a implementação do Nagios são: 1 máquina a correr um sistema operativo Linux ou variante Unix, e um compilador C.

3.4 Ntop

O Ntop - *Network Traffic Probe* [18] é uma aplicação simples, freeware e versátil baseada em *libpcap*, centrada na medição e caracterização de tráfego. Esta ferramenta foi inicialmente concebida por Luca Deri e Stefano Suin para detecção e resolução de problemas na rede do campus universitário da Universidade de Pisa, Itália.

O Ntop é capaz de mostrar a utilização da rede detalhando-a por host, protocolo, entre outros. Possui o seu próprio servidor web, permitindo o acesso aos resultados através de qualquer web browser e tem a capacidade de gerar excelentes gráficos o que facilita a interpretação de estatística de uso.

De certa forma, o NTOP pode ser visto como um simples agente RMON com um interface web embutido:

- Ordena o tráfego de rede de acordo com vários protocolos;
- Mostra o tráfego de rede ordenando-o de acordo com vários critérios;
- Disponibiliza graficamente estatísticas de tráfego;
- Guarda em disco estatísticas de tráfego persistente em formato RRD;
- Identifica a identidade (i.e. endereços de e-mail) de utilizadores;
- Identifica passivamente o sistema operativo dos hosts (i.e. sem enviar pacotes de probe);
- Mostra a distribuição do tráfego IP através dos variados protocolos;
- Analisa o tráfego IP e ordena-o de acordo com a fonte/destino;
- Mostra a *"Subnet Matrix"* do tráfego IP (quem está a falar com quem?);
- Reporta a utilização do protocolo IP ordenada pelo tipo de protocolo;
- Age como um colector NetFlow/sFlow para fluxos gerados por routers ou switches;
- Produz estatísticas de tráfego do tipo RMON;

Protocolos incluídos (configurável pelo utilizador):

- TCP/UDP/ICMP;
- (R)ARP;
- IPX;

- DLC;
- Decnet;
- AppleTalk;
- Netbios;
- TCP/UDP: FTP; Http; DNS; Telnet; SMTP/POP/IMAP; SNMP; NFS; X11;
- Fibre Channel;
    - Control Traffic - SW2,GS3,ELS;
    - SCSI;

Pontos de foco do NTOP:

- Medição de Tráfego;
- Monitorização de tráfego;
- Planeamento e optimização da rede;
- Detecção de violações da segurança da rede.

Na matéria da medição de tráfego o NTOP segue a utilização da rede, gerando variadas estatísticas para cada *"host"* existente na *subnet* local e para a *subnet* como um todo. A informação necessária é colectada pelo *"host"* que corre o NTOP através de uma simples observação do tráfego na rede. Este modo de funcionamento suaviza os requerimentos de processamento, dos nós operacionais para o host que está a correr o NTOP

Os requisitos de sistema para o Ntop são os seguintes: Unix (Linux, BSD, Solaris, MacOSX) ou MS Windows

Requisitos de Hardware (Segundo informações do fabricante):

- Memória: Depende da configuração do Ntop, nº de hosts, nº de sessões TCP Activas. De um modo geral pode ir desde poucos MB (redes pequenas) até 100 MB para uma WAN.

- CPU: Depende da configuração do Ntop, e condições de tráfego. Num PC moderno a operar numa rede de grandes dimensões, a carga de processador não ultrapassa os 10%.

3.5 CiscoWorks Lan Managment Solution

CiscoWorks não é uma ferramenta de gestão de rede mas sim uma família de aplicações organizadas em diversos pacotes de produtos (Tabela 2), que permitem aos administradores de rede facilmente aceder e gerir as avançadas funcionalidades da arquitectura CISCO. Estas ferramentas disponibilizam formas inovadoras, para centralizar a gestão de características críticas da rede de uma forma consistente, tais como disponibilidade, capacidade de resposta, resiliência, e segurança.

Gestão de elementos e Infraestruturas **(Routing and Switching Management)**
Cisco WorksLAN Management Solution
Gestão de acesso Wireless
CiscoWorks Wireless LAN Solution Engine (WLSE)
Configuração de redes e Gestão de alterações
CiscoWorks Network Compliance Manager
Gestão de Comunicações IP
Cisco Unified Communications Management
CiscoWorks Voice Manager
QoS Policy Management
CiscoWorks QoS Policy Manager

Tabela 2 – Família de aplicações CiscoWorks

A família de produtos Cisco Works é um exemplo de gestor de elementos, desenvolvida especificamente para a gestão de equipamentos Cisco. A utilização de gestores de elementos de rede, como o Cisco Works, não alivia necessariamente a necessidade de uma gestão a nível global de uma infra-estrutura de rede.

Um NMS, pode fornecer mapas de rede, visualização de alertas e eventos, e aceder à MIB de equipamentos de diversos fabricantes. Em complemento, a família de aplicações CiscoWorks pode, opcionalmente, ser integrada com alguns conhecidos NMSs, nomeadamente o *HP OpenView Network Node Manager*. Esta integração pode facilitar a utilização global dos recursos de um NMS, assim como das características específicas de um *Element Manager* para os equipamentos Cisco.

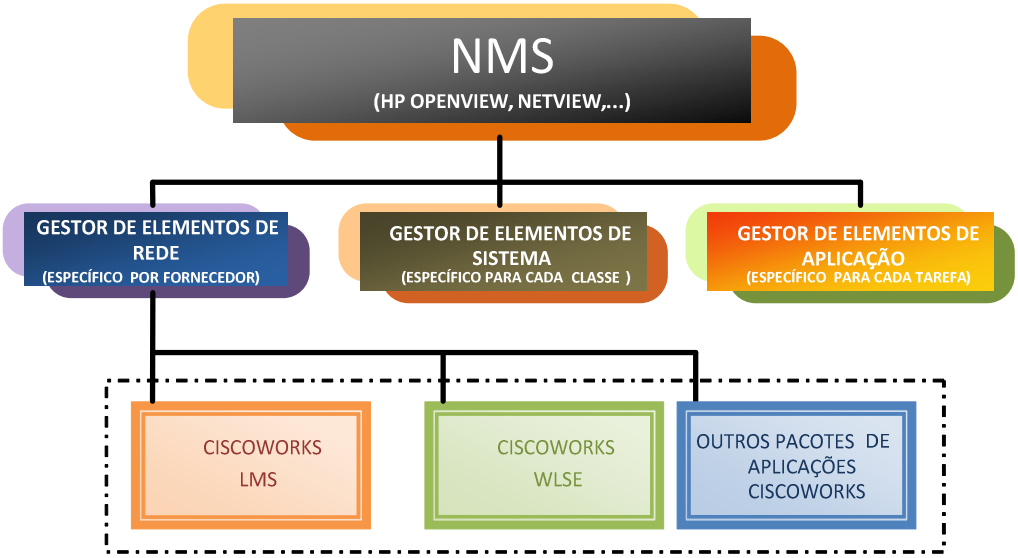


Figura 14 – Integração do CiscoWorks numa infra-estrutura de rede.

O CiscoWorks LAN Management Solution (LMS) [20] é o pacote de aplicações mais popular da família CiscoWorks e contém as funcionalidades para a gestão do equipamento activo numa rede. A sua arquitectura é baseada em clientes, servidores e agentes, que recorrem à informação disponibilizada pelas MIBs dos dispositivos Cisco geridos. A informação relativa a configurações, falhas e desempenho, pode ser adquirida através de diversos protocolos, conforme a situação ou especificidade da tarefa, estes englobam: SNMP, Telnet, RCP (remote copy protocol) e TFTP. A aquisição de dados é efectuada através de agendamento, manualmente, ou quando uma alteração na rede é detectada, sendo armazenada numa base de dados central. O acesso a esta informação,

por parte dos clientes, é efectuado através de browsers Web suportados. Uma mais-valia adicionada ao CiscoWorks é a integração com a extensiva base de dados de conhecimento da Cisco, pela qual é simplificado o processo de localização de informação relativa a produtos Cisco, imagens de software, actualizações de software, entre outros.

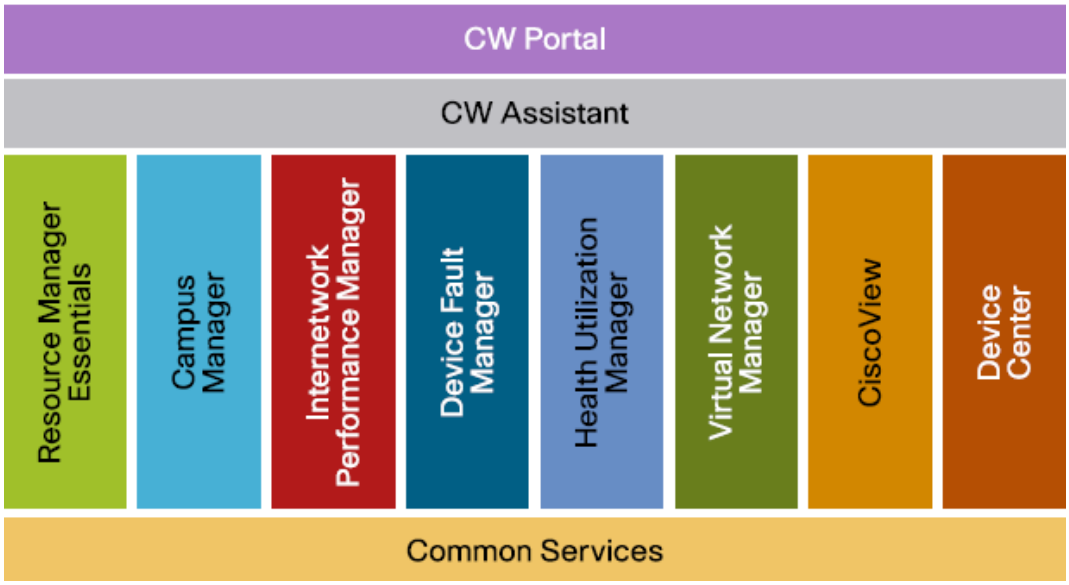


Figura 15 – CiscoWorks LMS 3.2

A versão actual do CiscoWorks LMS é a 3.2 [21] e engloba num pacote (Figura 15) um conjunto de aplicações alicerçadas numa gestão comum, acessíveis através de um interface Web flexível. Nos pontos seguintes são descritas as aplicações constituintes desta versão do CiscoWorks LMS, focando as vantagens que oferecem na gestão de uma rede Cisco:

- Documentação da rede
- Registo de alterações
- Implementação de actualizações
- Monitorização de desempenho
- Gestão de falhas
- Gestão configurações.

3.5.1 CiscoWorks LMS Portal

O CiscoWorks *LMS Portal* [22] é uma interface Web que permite a visualização de estatísticas importantes e detalhes das aplicações instalados no servidor, de uma forma centralizada, não sendo necessária a navegação para outra localização Web para visualizar a informação pretendida. Este ponto central, também permite o lançamento de aplicações para gerir e monitorizar os equipamentos de rede Cisco. O *LMS Portal* proporciona interfaces públicas e privadas. O portal público pode ser personalizado e será visto por todos os utilizadores do CiscoWorks. Por defeito, cada utilizador fica registado num portal privado, personalizável e de acesso restrito.

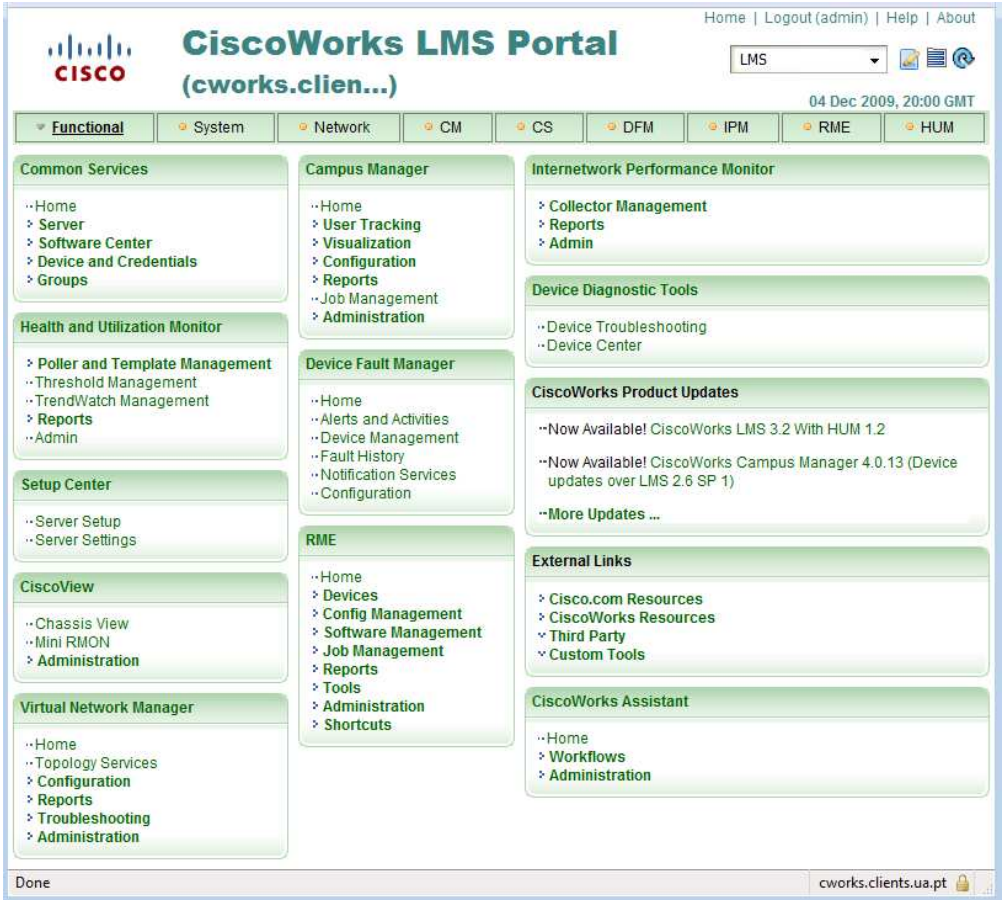


Figura 16 – CWLMS Portal

Views e *portlets* são as unidades básicas no LMS Portal (Figura 16). View é um método para exibir informações no portal. As *views* são exibidas como guias na parte superior da página. Os utilizadores têm a possibilidade de definir e guardar *Views* personalizadas.

Views incuídas por defeito:

- **Functional View**: fornece uma lista de aplicações e funções correspondentes.
- **System View**: Fornece um nível de visualização de alto nível, o estado do sistema de vários atributos de, incluindo o estado das tarefas, informações de backup, sistema de eventos de nível, e de aplicação com maior detalhe.
- **Network View**: Permite a visualização da rede e vários relatórios, para uma rápida resolução de problemas na rede.
- **Application Views**: Existe uma, para cada uma das aplicações instaladas no servidor.

.

3.5.2 CS - Commom Services

O CiscoWorks Common Services (CS) [22] é um conjunto de serviços de gestão (Figura 17), partilhado pelas várias aplicações de gestão:

- Serviços de RunTime: interface Web, gestão de processos, segurança, e o motor de ajuda.
- Serviços de Sistema: Base de dados e utilitários; serviços de distribuição de eventos e gestão de tarefas.
- Serviços de Core: serviços de apoio ao centro de gestão de aplicações

Figura 17 – Estrutura do CiscoWorks Common Services

Disponibiliza um ambiente centralizado da infra-estrutura de aplicações para todas as soluções de gestão de rede existentes no CWLMS. Tem o objectivo de possibilitar a partilha de um modelo comum para o armazenamento de dados, contas de utilizador (funções e permissões associadas) e protocolos de segurança.

Define uma navegação central e um modelo para o lançamento das aplicações com o intuito de padronizar a utilização de todas as funções de gestão, a integração multi-nível das aplicações, e a infra-estrutura base para a integração com aplicações de terceiros.

O Common Services pode ser utilizado para realizar a descoberta dos equipamentos de rede Cisco a partir da especificação de dispositivos de

referência. À medida que os equipamentos vão sendo descobertos, a identificação e informação associadas são armazenadas no repositório de dispositivos e credenciais, o DCR (Device and Credential Repository). O DCR guarda todo o tipo de credenciais, tais como as *community strings* SNMP e as passwords de acesso aos equipamentos para utilização futura pelas aplicações do CWLMS. O CS disponibiliza também ferramentas que permitem a configuração do servidor, gestão do DCR, administração de grupos, e a actualização das aplicações do CWLMS e sistema operativo dos equipamentos.

Agregadas à instalação do CS são instaladas as aplicações LMS Setup Center e Device Center:

- O LMS **Setup Center** disponibiliza uma localização centralizada para a configuração do sistema, segurança, armazenamento de dados, calendarização da recolha de dados, e definições de eliminação da informação armazenada.
- O **Device Center** disponibiliza a sumarização da informação dos equipamentos de rede, ferramentas que possibilitam a detecção e resolução de problemas, tarefas de gestão, e relatórios de cada dispositivo.

Na presença de problemas na rede, a navegação pelos diversos menus do CiscoWorks para procurar uma ferramenta que permita a realização de diagnósticos, pode ser penosa. Uma aplicação pode criar entropia pelo facto de requerer, para a realização de uma tarefa, o acesso menus que se encontram noutra localização. Por vezes, a depuração de um comportamento invulgar de um equipamento, é facilitada se existir a possibilidade de começar a partir de um dispositivo e visualizar as ferramentas disponíveis para a realização da tarefa. O Commom Services segue esta filosofia.

3.5.3 CWA - CiscoWorks Assistant

O CiscoWorks Assistant (CWA) [24] é uma ferramenta Web que disponibiliza Workflows (fluxos de trabalho). Estes Workflows são uma compilação de tarefas necessárias, à instalação dos servidores CiscoWorks LMS, e à identificação e resolução de problemas em equipamentos de rede.

Workflows existentes no CWA:

- **Server Setup:** executa tarefas de configuração em servidores e dispositivos.
- **End Host/IP Phone Down:** Permite a identificação de e resolução de problemas equipamentos de telefonia IP.
- **Device Troubleshooting:** facilita a identificação de dispositivos sem conectividade.

O CWA é instalado juntamente com o CiscoWorks Common Services e o LMS Portal.

3.5.4 CM - Campus Manager

O objectivo principal do Campus Manager [25] é a gestão de configurações da conectividade física e lógica entre dispositivos de rede e estações de trabalho. Consiste num conjunto de ferramentas Web que disponibilizam: vários tipos de visualizações gráficas da topologia de rede, informação relativa a utilizadores e um ambiente gráfico para configuração de VLANs, LANEs e portas dos equipamentos. Também possui uma capacidade avançada de gestão dos protocolos de Spanning Tree.

Embora o Campus Manager seja um componente integral no CWLMS, também pode ser utilizado isoladamente como uma solução de gestão que facilita a configuração, compreensão e visualização da complexa infra-estrutura da 2ª camada de rede.

As aplicações que integram o Campus Manager são as seguintes:

- **Topology Services:** Faz a auto-descoberta de switches e routers Cisco, e gera mapas da topologia de rede que facilitam a identificação do tipo de dispositivos e a forma como se encontram conectados entre si. Adicionalmente também faz a auto-descoberta de domínios ATM e VTP, e VLAN *"memberships"* configurados na rede. Entre as diversas funcionalidades do Topology Services, destacam-se também o interface gráfico para configuração de VLANs, LANEs e serviços ATM, e a sinalização visual automatizada de problemas físicos e lógicos com a configuração de rede.

- **User Tracking:** identifica os dispositivos finais ligados a equipamentos Cisco descobertos na rede, incluindo impressoras, telefones VOIP, servidores e maquinas cliente, fornecendo informação detalhada relativa a: endereço Mac, endereço IP, nome DNS, nome netbios, portas atribuídas, VLAN membership, etc. Também colecta (através de configuração especifica) o nome dos utilizadores associados a estações de trabalho, a partir de hospedeiros UNIX, controladores de domínio Windows (PDC), e serviços de directório Novell (NDS), facilitando a tarefa de localizar utilizadores na rede.

- **VLAN, PVLAN, and VTP Management:** fornece um acessível interface gráfico para a configuração de VLANs e LANEs, e atribuição portas de switches a VLANs.

- **Discrepancies and Best Practices Deviations:** disponibiliza relatórios acerca de discrepâncias, tais como inconsistências, anomalias ou configurações inapropriadas na rede descoberta. Estes relatórios também incluem desvios relativos a boas práticas, problemas que embora não causem um impacto relevante na rede, informam acerca de diferenças entre as configurações implementadas e praticas normais ou recomendadas de implementação.

- **VNM - Virtual Network Manager**: Esta aplicação complementa o Campus Manager, funcionando em conjunto com este e com o RME, alargando as funcionalidades de gestão pela introdução de pré-provisionamento, provisionamento e monitorização de VRF (Virtual Routing and Forwarding). O VNM é uma solução corporativa que permite aos administradores de rede configurar e editar as configurações VRF assim como a recolha de detalhes dos dispositivos suportados, de forma a serem gerados relatórios acerca de disponibilidade de VRF e configurações implementadas.

3.5.5 RME - Resource Manager Essentials

O objectivo principal do RME [26] é a gestão de configurações. Contém diversas funcionalidades automatizadas que simplificam as tarefas de configuração dos equipamentos, como a realização de actualizações de software e a alteração dos ficheiros de configuração em múltiplos dispositivos. O RME também inclui funcionalidades enquadradas na gestão de falhas, através da sua capacidade para filtragem de mensagens de Syslog.

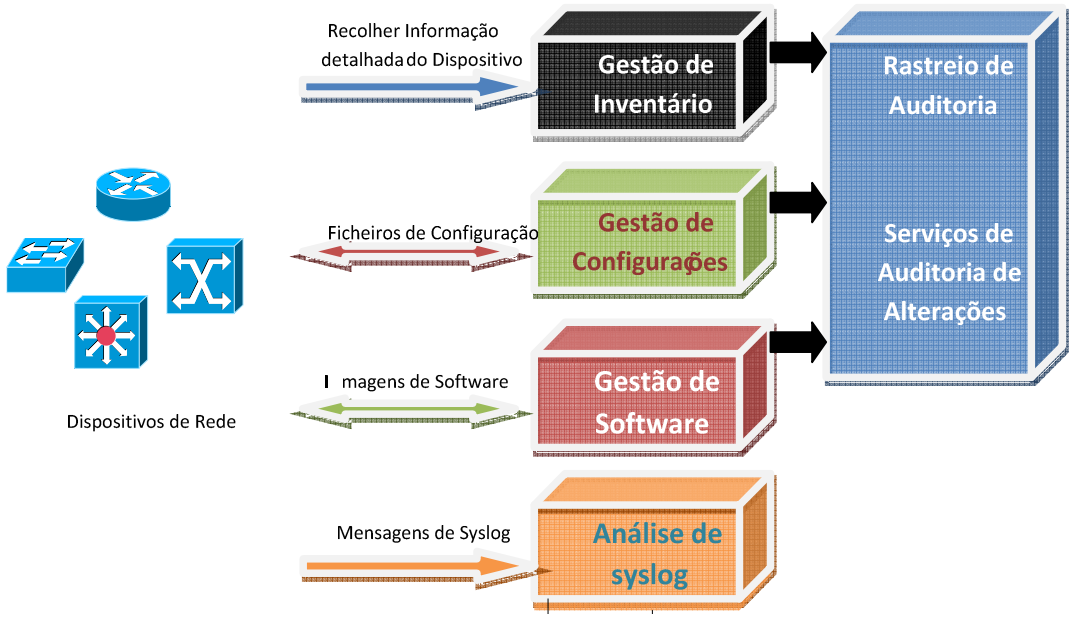


Figura 18 – Funcionalidades do RME

Entre as diversas funções atribuídas ao RME, destacam-se as seguintes (Figura 18):

- **Gestão de Inventário:** recolhe e guarda informação detalhada acerca de todos os dispositivos geridos pelo RME, e disponibiliza-a a através de um conjunto extensivo de relatórios nativos ou personalizáveis. Em conjunção com os serviços de auditoria de alterações, detecta automaticamente alterações efectuadas nos equipamentos.

- **Gestão de configurações:** guarda as versões correntes e anteriores dos ficheiros de configuração de todos os dispositivos existentes no inventário do RME. Detecta automaticamente alterações efectuadas na configuração dos equipamentos e actualiza o arquivo de configurações no caso de estas ocorrerem. Disponibiliza duas ferramentas adicionais, *NetConfig* e *Config Editor* para edição de ficheiros de configuração:
    - **NetConfig:** permite a configuração de um conjunto de comandos para execução de configurações em múltiplos dispositivos em simultâneo.
    - **Config Editor:** permite a edição de ficheiros de configuração através de um interface gráfico, e possibilita a recolha individual de ficheiros que se encontram nos equipamentos

- **Gestão de software:** guarda uma cópia das imagens de software que se encontram em produção, assim como outras que o administrador rede deseja manter. Executa a actualização de imagens de software em múltiplos dispositivos ao mesmo tempo, e permite a recuperação para as versões anteriores no caso ocorrerem erros no processo de actualização. Opcionalmente, para o controlo de gestão de alterações e segurança, é possível restringir as permissões a utilizadores para a realização da recolha das imagens de software.

- **Análise de syslog:** guarda as mensagens de syslog enviadas pelos dispositivos e permite a personalização de filtros por tipo de mensagem. Possibilita também a configuração de comandos a executar automaticamente, no caso da detecção de mensagens especificas, como por exemplo, o envio de notificações por email na ocorrência de erros críticos.

- **Serviços de auditoria de alterações:** Efectuam o rastreio de alterações efectuadas a diversos componentes funcionais da rede. Estes serviços guardam informação detalhada acerca de qualquer tipo de alterações efectuadas no inventário, imagens de software e ficheiros de

configuração dos equipamentos de rede. A informação armazenada facilita o diagnóstico de problemas ocorridos na realização de alterações, permitindo a identificação das mesmas, como e quando foram realizadas, e quem as efectuou. Adicionalmente possibilita a filtragem de registos por tipo, utilizador, data, ou método de alteração (telnet, rcp, etc.).

- **Rastreio de auditoria:** Rastreia e gera relatórios de alterações efectuadas no servidor RME, realizadas pelo administrador.

3.5.6 IPM - Internetwork Performance Monitor

IPM [27] é uma aplicação que proporciona capacidade para a medição de tempos de resposta na rede, determinação de disponibilidade, e análise de padrões de tempos de resposta em ligações ponto a ponto e “hop by hop”. Também tem a capacidade para gerar alarmes relativos a atrasos de longa duração pelo processamento de traps SNMP, assim como gerar eventos que facilitam a resolução proactiva de potenciais problemas de desempenho antes que estes afectem os utilizadores da rede, disponibilizando relatórios em tempo real ou de carácter histórico.

O recurso tradicional a Pings para medição de tempos de resposta pode não ser suficiente numa Gestão de Desempenho avançada. A medição de atrasos relacionados com protocolos tais como TCP, UDP, DNS, DHCP, permite a obtenção de informação essencial para a optimização da rede.

A medição de desempenho do tráfego gerado pelas aplicações existentes numa rede, efectuada pelo IPM, é realizada directamente no mesmo, o que apresenta vantagens na precisão das medidas de tempos de resposta. O IPM utiliza a tecnologia Cisco IOS IP SLA para monitorizar o desempenho ponto a ponto de redes multi-protocolares. A utilização desta tecnologia permite a medição de cinco tipos de estatísticas de desempenho de rede fundamentais: latência, disponibilidade, jitter, perda de pacotes, e erros.

3.5.7 DFM - Device Fault Manager

O Device Fault Manager [28] oferece monitorização em tempo real da robustez operacional da rede. Utiliza diversos mecanismos para detectar e isolar falhas, que obedecem a regras pré-definidas de identificação de problemas, baseadas em conhecidas condições problemáticas. O engenho de “polling” e análise do DFM, já vem configurado com os parâmetros relativos à informação a recolher, referente a valores aceitáveis, para a determinação da ocorrência de falhas.

O DFM encontra-se habilitado para receber traps SNMP, e consultar as variáveis MIB pré-definidas, da maioria dos equipamentos Cisco. A partir destas capacidades, correlaciona múltiplos eventos e disponibiliza a informação resultante sob a forma de alertas, evitando a intervenção directa nos dispositivos para a determinação do estado de operacionalidade.

Possibilita também a personalização das notificações geradas, de forma a proactivamente disponibilizar alertas referentes a problemas existentes na rede, facultando a filtragem do histórico de falhas por alertas ou eventos. Os alertas gerados pelo DFM são baseados na informação obtida a partir dos seguintes métodos:

- **Polling:** Identifica condições que garantem a ocorrência de um evento, tais como dispositivos sem conectividade ou interfaces inactivos.
- **Tresholds:** Compara os dados recolhidos dos dispositivos, com limiares de operação aceitáveis, gerando eventos apropriados à ocorrência de valores limite excedidos.
- **SNMP traps:** processa as traps SNMP, enviadas pelos dispositivos para o porto standard (UDP 162) ou para um porto especificado.

O histórico de falhas guardado pelo DFM, permite a visualização de actividade ocorrida durante 31 dias, e incluí alertas, eventos e anotações efectuadas pelo administrador.

3.5.8 CiscoView

Cisco View [29] é uma aplicação gráfica que permite a configuração e monitorização de equipamentos cisco. A peculiaridade desta ferramenta é a visualização física dos dispositivos, que disponibiliza o estado das portas através de códigos de cores, e facilita a percepção rápida de informação essencial.

.

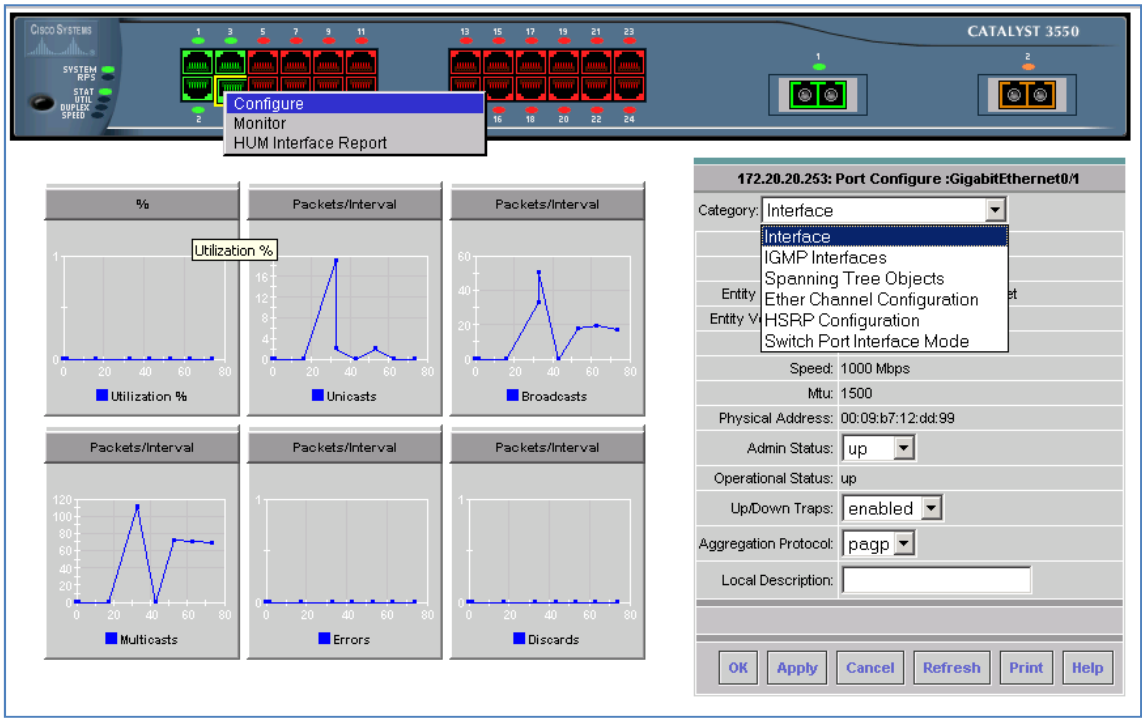


Figura 19 – Cisco View

Utiliza SNMP v2/v3 para recolher as informações de configuração e desempenho dos dispositivos. Os dados recolhidos são utilizados para providenciar visualizações em tempo real do estado físico e lógico, e monitorização estatística. Adicionalmente pode ser utilizado para modificação das configurações dos dispositivos.

As funcionalidades do Cisco View permitem o seguinte:

- Representação gráfica de dispositivos, incluindo o estado de componentes, tais como, interfaces, fonte de alimentação e leds.
- Configuração de parâmetros de operação dos dispositivos

- Monitorização estatística de interfaces, utilização de recursos e desempenho
- Realização de operações específicas a cada tipo de dispositivo.
- Gestão de grupos de dispositivos agregados.

Mini-RMON Manager

A aplicação Mini-RMON manager encontra-se integrada no CiscoView e é uma ferramenta para monitorização remota em tempo real, que permite a configuração RMON dos equipamentos, recolha de dados relativos a estatísticas Ethernet e a configuração de limiares aceitáveis de funcionamento. São gerados alertas sempre que esses limiares sejam ultrapassados o que facilita o diagnóstico e melhora a disponibilidade da rede.

3.5.9 HUM - Health and Utilization Monitor:

CiscoWorks Health and Utilization Monitor [30] é uma aplicação baseada em SNMP que monitoriza elementos de rede, tais como processadores, memória, interfaces, ligações, entre outros, para métricas de disponibilidade e utilização, e tendências históricas. O HUM pesquisa as variáveis MIB dos dispositivos através de SNMP para recolher informação útil à criação de relatórios de carácter historial e corrente, que permitem a análise e níveis de utilização e disponibilidade dos dispositivos de rede. Estes relatórios podem ser, disponibilizados por correio electrónico, guardados ou imprimidos para futura referência.

É uma aplicação pré-integrada no CiscoWorks LMS 3.2 e distribuída como parte do mesmo pacote de software. Foi desenhada com a característica de *add-on* e encaixa-se em pleno com as restantes aplicações do LMS.

As funcionalidades de destaque do HUM são as seguintes:

- Suporte para integração com o Cisco Works LMS 3.2
- Suporte para monitorização da funcionalidade Power-over-Ethernet (PoE) em equipamentos Cisco que a suportam.
- Análise de tendências para identificação de padrões de desempenho da rede
- Produção de gráficos para uma rápida análise comparativa de pontos de informação assim como o consumo de recursos relativo.
- Configuração de thresholds e notificações em tempo real.
- Portlet de histogramas com capacidade para exportação de informação
- Portlet Live-GraphIt que permite o diagnóstico em tempo real de problemas de desempenho.
- Suporte para análise de traps e syslog

3.5.10 Licenciamento

O CiscoWorks LMS é um produto comercial, para o qual existem cinco tipos de licenciamento baseados, em número de equipamentos e colectores. (Tabela 1)

	RME	CM	DFM	IPM	
	Dispositivos				Colectores
CWLMS-3.2-100-K9	100	100	100	100	300
CWLMS-3.2-300-K9	300	300	300	300	1000
CWLMS-3.2-1.5K-K9	1500	1500	1500	1500	1500
CWLMS-3.2-5K-K9	5000	5000	5000	5000	5000/10000*
CWLMS-3.2-10K-K9	10000**	5000	5000	5000	5000/10000*
*a opção de 10000 colectores é condicionada por 1 hora de polling **o RME não foi testado com opção de 10000 dispositivos em implementações de servidor único, pelo que é direccionado a ambiente multi-server					

Tabela 3 – CWLMS, Licenciamento

3.5.11 Requisitos de hardware e software

O CiscoWorks LMS 3.2 é suportado pelos seguintes sistema operativos (Tabela 4):

Sun Microsystem Solaris	Solaris 8 Solaris 9 Solaris 10
Microsoft Windows	Windows Server 2003 SE/EE Windows Server 2003 R2 SE/EE Windows Server 2003 SE/EE SP1/SP2 Windows Server 2003 R2 SE/EE SP1/SP2 Windows Server 2008 SE/EE SP1/SP2 32/64-bit
Sistemas de Virtualização	VMware ESX server 3.0.1 VMware ESX Server 3.5.0 VMware ESXi 3.5 Update 2 VMWare ESX 4.0 VMWare ESXi 4.0 Hyper V Virtualization

Tabela 4 – CWLMS, requisitos de sistema (servidor)

Quanto ao requisitos de hardware o cenário muda de figura em consonância com o tipo de licenciamento, ou seja, o número de equipamentos a serem geridos. A tabela (Tabela 5) mostra as recomendações de hardware fornecidas pela Cisco.

SKU	Solaris	Microsoft Windows
CWLMS-3.2-100-K9	N/A	1 CPU ; 2 GB RAM ; 4 GB swap
CWLMS-3.2-300-K9	Solaris 9: 1 CPU ; 2 GB RAM ; 4 GB swap Solaris 10: 1 CPU ; 4 GB RAM ; 8 GB swap	1 CPU ; 2 GB RAM ; 4 GB swap
CWLMS-3.2-1.5K-K9	2 CPUs ; 4 GB RAM ; 8 GB swap	2 CPUs a 3.66 GHz ; 4 GB RAM ; 8 GB swap
CWLMS-3.2-5K-K9	Servidor único para todas as aplicações do LMS até 5000 equipamentos: 4 CPUs ; 8 GB RAM ; 16 GB swap	Servidor único para todas as aplicações do LMS até 5000 equipamentos: 4 CPUs ; 8 GB RAM ; 16 GB swap
CWLMS-3.2-10K-K9	Servidores dedicados a cada aplicação: 2 CPUs ; 4 GB RAM ; 8 GB swap	Servidores dedicados a cada aplicação: 2 CPUs ; 4 GB RAM ; 8 GB swap
Disco rígido	100/300 equipamentos: 25 GB 1500/5000/10,000 equipamentos: 35 GB	100/300 equipamentos: 25 GB 1500/5000/10,000 equipamentos: 35 GB
CPU	• UltraSPARC III • UltraSPARC IIIi processor • UltraSPARC IV processor • UltraSPARC IV+ processorUltraSPARC T1 processor • UltraSPARC T2 processor • UltraSPARC T2+ processor(only onSolaris 10) • SPARC64 VI processor(only onSolaris 10) • Sparc64 VII processor(only onSolaris 10)	**Processadores Intel** • Intel Xeon (Dual Core) • Intel Core Duo T2600 - T2300 • Intel Pentium Extreme Edition 965 (Dual Core) • Intel Pentium D 960 (Dual Core) • Intel Pentium 4 com Hyper-Threading • Quad Core Intel Xeon • Intel Itanium • Intel-VT (VMWare Optimized hardware) • Quad-Core Intel Xeon 5400/5300/7300 series **AMD processors** • Dual-Core AMD Opteron • AMD Opteron • AMD Athlon 64 FX • AMD Athlon 64 X2 Dual-Core • AMD -V

Tabela 5 – CWLMS, requisitos de hardware (servidor)

As máquinas cliente de suporte ao CiscoWorks LMS, também têm recomendações mínimas de hardware e software para a operação do Interface gráfico (Tabela 6).

Disco	• Solaris: 1 GB swap • Windows: 1 GB de memória virtual
Memória	512 MB
Sistema operativo	• IBM PC- Intel Pentium IV • Windows 2003 SE/EE SP2 (32 e 64 Bit) • Windows 2003 SE/EE R2 SP2 (32 and 64 Bit) • Windows XP SP2/SP3 • Windows Vista Business Edition (Apenas versão Inglesa e Japonesa) • Windows 2008 SE/EE (32 e 64 bit) • Solaris 9, Solaris 10 (Apenas versão Inglesa e Japonesa)
Browser	• Internet Explorer 6.0. SP2-Windows Server 2003, Windows XP SP2 • Internet Explorer 7.0 (Windows Vista, Win XP SP2, e Windows 2003) • Firefox 3.X para Windows e Solaris • Firefox 2.X para Solaris 9

Tabela 6 – CWLMS, requisitos mínimos (clientes)

3.6 Conclusões

Os sistemas de gestão e monitorização abordados seguem linhas de funcionamento e operação distintas, e não foi intenção efectuar um estudo comparativo. Todos eles podem representar um papel importante numa infra-estrutura de rede e englobam no seu conjunto as áreas funcionais de gestão referidas pelo modelo FCAPS.

Quanto à integração com ITIL, nenhuma das ferramentas está direccionada à gestão dos seus processos, mas podem ser vantajosas na execução de tarefas e fornecimento de informações fundamentais para a sua implementação. Particularmente, o CiscoWorks LMS em conjunto com outro produto CiscoWorks, o *CiscoWorks Network Compliance Manager*, pode apresentar uma solução completa para a implementação das normas ITIL em Gestão de redes.

A Tabela 7 mostra um mapeamento das ferramentas apresentadas nas áreas funcionais do modelo FCAPS e em alguns dos processos do modelo ITIL.

		Cacti	Ntop	Nagios	CWLMS
FCAPS	Fault Management	✓	✓	✓	✓
	Configuration Management	✓			✓
	Accounting Management	✓	✓	✓	✓
	Performance Management	✓			✓
	Security Management		✓		✓
ITIL	Incident Management				✓
	Problem Management	✓	✓	✓	✓
	Change Management				✓
	Realease Management				✓
	Configuration Management	✓			✓
	Avaiability Management	✓	✓	✓	✓
	Service level Management				✓
	Service reporting	✓	✓	✓	✓

Tabela 7 – Enquadramento com os modelos de Gestão de Redes.

Embora a avaliação das ferramentas de gestão e monitorização, deva ser baseada essencialmente num estudo teórico de todas as características pertinentes, é imprescindível a experimentação prática em ambientes apropriados que permitam a interacção humana com as tecnologias analisadas.

4 Implementação dos sistemas de gestão

4.1 Introdução

A análise prática de tecnologias e ferramentas que suportam as áreas funcionais da gestão de redes, é fundamental para a avaliação das potencialidades disponibilizadas em complementação a um estudo teórico efectuado. Esta análise deverá focar-se em necessidades pertinentes que as organizações experienciam, no planeamento e manutenção da estrutura de rede.

O ambiente diversificado que constitui a rede informática da Universidade de Aveiro, é sustentado por aproximadamente 500 equipamentos activos, sendo a sua maioria de marca Cisco. Atendendo ao emergente crescimento das TI, é de todo o interesse encontrar soluções que automatizem a gestão e monitorização dos equipamentos activos, com o objectivo de minimizar prejuízos de produtividade, causados pela complexidade inerente e situações problemáticas. De forma análoga, o recurso a ferramentas de monitorização e análise estatística de tráfego, essencial para a gestão de desempenho da rede, deverá ser optimizado através da avaliação de novas funcionalidades, apresentadas nas versões actuais das aplicações utilizadas.

O CICUA, responsável pela gestão da infra-estrutura de comunicações e suporte informático da Universidade de Aveiro, disponibilizou no âmbito deste estudo, o seu laboratório de testes assim como equipamentos de rede, servidores, acesso à rede de “staging”, para a montagem do cenário escolhido para a implementação dos sistemas estudados.

Este capítulo, aborda a implementação das ferramentas estudadas, em ambiente laboratorial, num cenário orientado à arquitectura Cisco, em termos de topologias de rede e tecnologias utilizadas.

4.2 Implementação laboratorial

Atendendo aos requisitos mínimos de hardware necessários para a implementação dos sistemas estudados, foram disponibilizadas duas máquinas com as características apresentadas na Tabela 8.

	Servidor 1	Servidor 2
ref.	Dell PowerEdge 1850	HP Compaq ProLiant DL360
CPU	Intel Xeon 3.0 GHz (duplo)	Intel Pentium III 1.2GHz
RAM	2 GB	1.5 GB
SO	MS Windows 2003 server SE SP2	MS Windows 2000 server SP4

Tabela 8 – Caracteristicas dos servidores implementados em laboratório

Para o CiscoWorks LMS foi atribuído o Servidor 1, devido este sistema necessitar de mais recursos de hardware em relação às restantes ferramentas. No Servidor 2 foram implementadas as ferramentas Nagios, Cacti e Ntop, assim como um serviço de DNS para integração com a rede de testes. Para possibilitar o que foi designado para o Servidor 2, recorreu-se à aplicação VMware Server 2.0, de forma a virtualizar os sistemas operativos que alojaram os serviços mencionados anteriormente (Tabela 9).

<table>
<tr><td></td><td colspan="3">Vmware Server 2.0</td></tr>
<tr><td>Sistemas virtualizados</td><td>Ubuntu Server 8.04</td><td>CentOS Server 4.7</td><td>MS Windows XP SP3</td></tr>
<tr><td>Memória RAM atribuída</td><td>384 MB</td><td>512 MB</td><td>384 MB</td></tr>
<tr><td rowspan="3">Aplicações</td><td>Bind 9</td><td rowspan="3">Cacti 0.87c</td><td rowspan="3">Plugins de integração com o Nagios e CWLMS</td></tr>
<tr><td>Nagios 3</td></tr>
<tr><td>NTOP 3.3</td></tr>
</table>

Tabela 9 – Virtualização de sistemas.

A instalação e configuração dos servidores tiveram a seguinte ordem de execução:

Servidor 1

- Instalação do MS Windows 2003 server e actualizações respectivas.
- Instalação do CiscoWorks LMS. Durante o percurso da execução desta dissertação foram instaladas três versões do LMS, devido primeiramente ao facto de a versão 3.0 ser a única disponível na altura da implementação do cenário. Pouco tempo depois, conseguiu-se a versão 3.1 que substituiu a anterior. Por fim, a Cisco disponibilizou para download a última e actual versão, a 3.2, tendo o estudo incidido sobre esta.

Servidor 2

- Instalação do MS Windows 2000 server e actualizações
- Instalação e configuração do VMware server 2.0
- Criação de máquinas virtuais
    - Instalação e configuração do Ubuntu 8.04
        - Instalação e configuração do Bind 9
        - Instalação e configuração do Ntop 3.3
        - Instalação e configuração do Nagios 3
    - Instalação e configuração do CentOS 4.7
        - Instalação e configuração do Cacti 0.87c

Adicionalmente instalou-se uma máquina cliente com Windows XP SP3 (virtualizada no servidor 2) para realização de testes associados à implementação dos sistemas de monitorização e gestão.

A Figura 20 apresenta o cenário geral da implementação. Ambos os servidores foram configurados de forma a terem conectividade com a rede de testes (isolada) e a rede de *staging*, dando a possibilidade para acederem à internet e à rede da UA, assim como a experimentação em ambiente real.

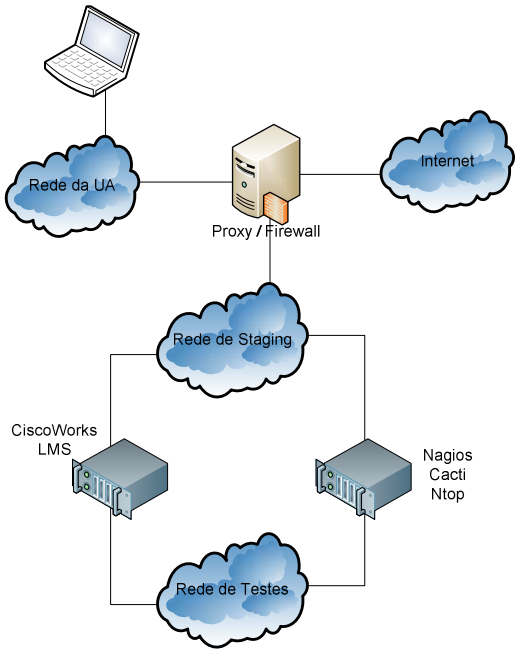


Figura 20 – Cenário da implementação laboratorial.

A montagem da rede de testes (Figura 21) foi baseada num modelo de rede hierárquico, com três níveis redundantes: core, distribuição e acesso.

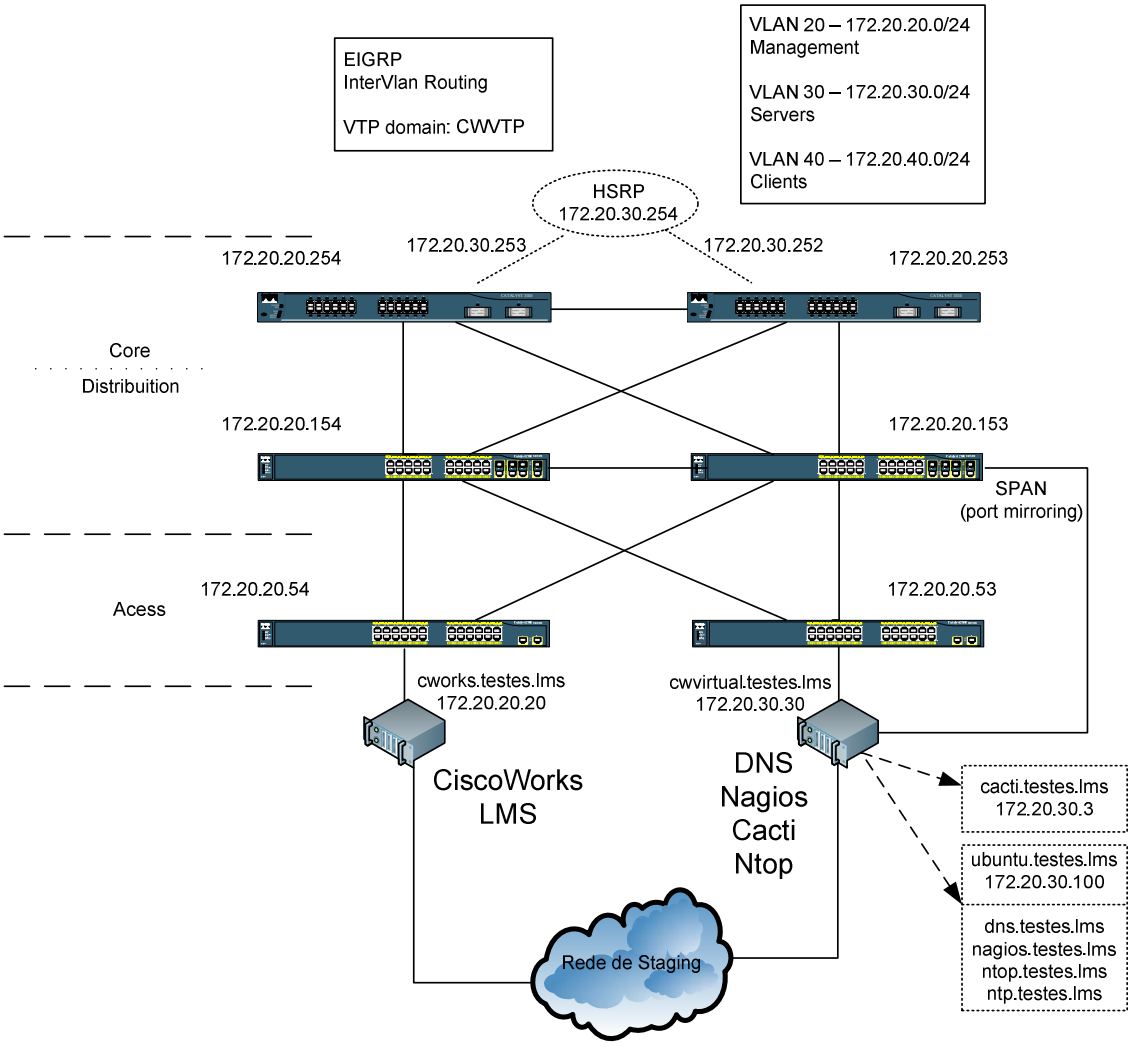


Figura 21 – Rede de testes

A Figura 21 resume as configurações de rede efectuadas nos equipamentos assim como os serviços implementados.

4.2.1 CiscoWorks LMS

A instalação e configuração do CiscoWorks requereram algum planeamento. Seguindo as recomendações fornecidas pela Cisco [23] foi posto em prática o fluxo de trabalho apresentado na Figura 22.

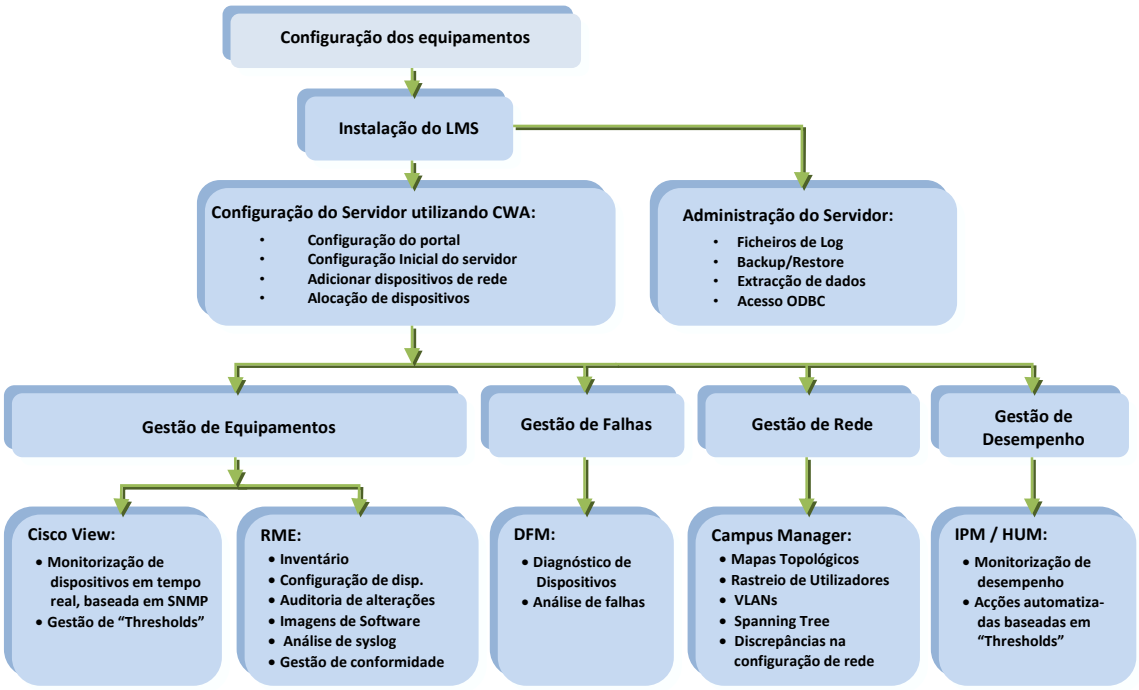


Figura 22 – Fluxo de trabalho para a implementação do CiscoWorks LMS

Antes de avançar com instalação do CiscoWorksLMS foi necessário realizar a configuração prévia dos equipamentos de rede, nomeadamente a activação do protocolo CDP (Cisco Discovery Protocol), configuração SNMP, e credencias de acesso aos dispositivos tais como Telnet, SSH, ligação à consola (CLI), entre outras.

De seguida foi instalado o servidor CWLMS, e efectuado o setup inicial que inclui as definições do interface de utilizador, verificação e modificação de configurações definidas por defeito para as várias aplicações, criação de

contas de utilizador com permissões suficientes para a execução das diversas tarefas, o estabelecimento da comunicação segura entre os clientes e o servidor, etc. Concluída a preparação inicial do servidor e equipamentos, procedeu-se à adição manual de dispositivos e à descoberta automática da rede de forma a popular o DCR (repositório de dispositivos e credenciais); durante este processo toda a informação relacionada com credenciais e acesso a dispositivos, é armazenada no DCR, alocando os equipamentos de forma que outras aplicações os possam gerir, através da sincronização automática da base de dados de dispositivos de cada aplicação com o DCR. As aplicações envolvidas na configuração inicial foram: LMS Portal, CiscoWorks Assistant, Common Services, and Setup Center.

4.2.1.1 Configuração inicial dos equipamentos

Para que as funções de gestão do LMS funcionem correctamente, é necessário preparar os equipamentos de forma que estes consigam comunicar com o servidor. Dando como exemplo as *community strings* SNMP definidas no servidor, deverão ser iguais às configuradas nos dispositivos.

Seguindo as recomendações do fabricante, foram efectuadas as seguintes configurações nos equipamentos (switches):

- Configurações genéricas:
  - ✓ System Name: O nome do sistema de cada equipamento (Cisco IOS) na rede, deverá ser único
  - ✓ Domain Name (nos sistemas cisco (Cisco IOS), o nome de domínio afecta o nome de sistema)
  - ✓ Command-Line Prompts (acesso à linha de comandos)
- Protocolos de comunicação
  - ✓ SNMP - definições implementadas em diferentes equipamentos:
    - SNMPv1/v2c,
    - SNMPv3: modos AuthNoPriv e AuthPriv
    - Traps
  - ✓ System Reload:

- ✓ Telnet/SSH -
- ✓ Remote Copy Protocol:
- ✓ HTTP

- Outros
  - ✓ CDP
  - ✓ Syslog

4.2.1.2 Configuração inicial do servidor (LMS)

Todas as recomendações indicadas na documentação disponível foram seguidas para a configuração inicial do servidor.

Recorrendo à ferramenta Cisco Works Assistant destacam-se a realização das seguintes tarefas:

- Configuração de credenciais, e protocolos de comunicação.
- Configuração do modo de gestão (automatizado ou manual)
- Auto descoberta da rede
- Alocação dos equipamentos às aplicações do LMS (RME, CM, DFM, IPM)

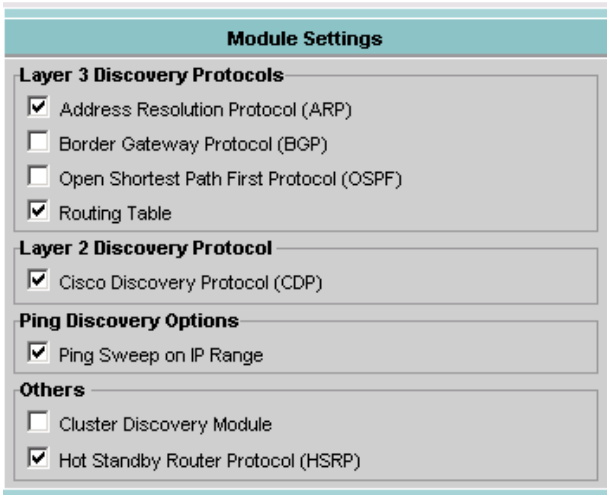


Figura 23 – protocolos para descoberta da rede

A descoberta automática da rede é suportada por diversos protocolos de 2ª e 3ª nível (Figura 22), embora a o utilizado preferencialmente é o protocolo CDP que se encontra implementado em todos os equipamentos Cisco. A Figura 24 apresenta o método de descoberta utilizado pelo LMS através de CDP.

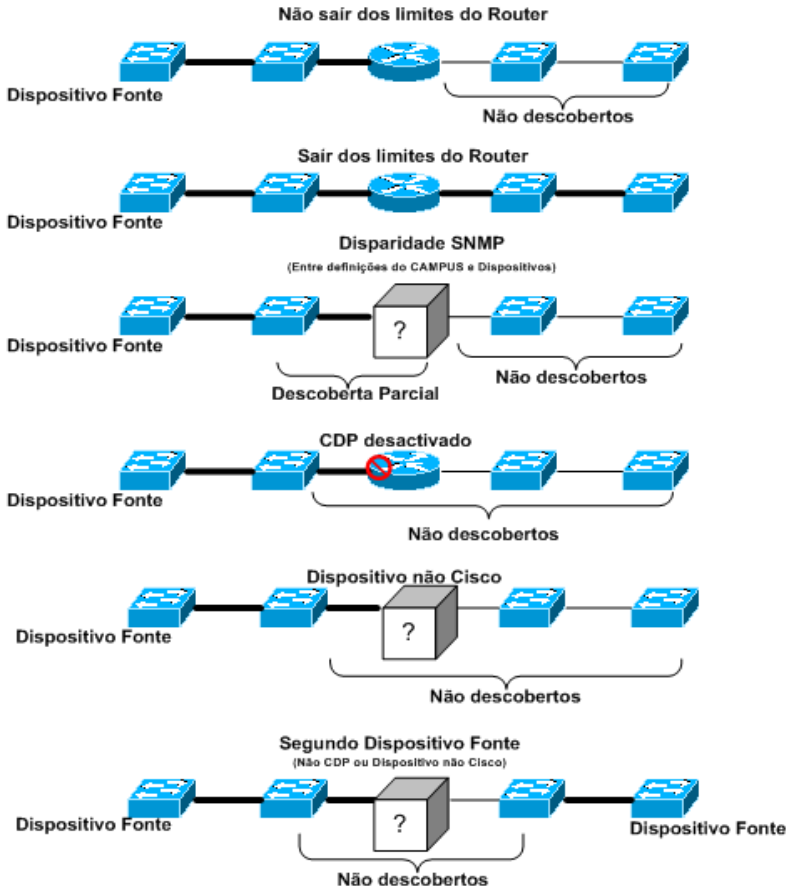


Figura 24 – descoberta da rede por CDP

O LMS 3.2 suporta a configuração de múltiplos conjuntos de credenciais a serem aplicados durante a adição, edição e importação de dispositivos. A criação de políticas aplicadas a credenciais permite a aplicação das mesmas a conjuntos de dispositivos definidos por, gamas IP, nome de visualização ou nome de hosts.

Durante a configuração inicial, também foram efectuadas tarefas para criação de utilizadores e integração na AD na Universidade de Aveiro, permitindo a a atribuição de permissões de acesso a contas de Utilizador Universal (Contas do domínio ua.pt).

4.2.1.3 Gestão de equipamentos

As aplicações Resource Manager Essentials (RME), CiscoView e Device Center, foram desenhadas particularmente para a gestão de elementos, e fornecem utensílios que facultam soluções, para questões levantadas no planeamento e manutenção de redes. Deste modo, visando o cenário implementado e as necessidades implícitas na gestão dos equipamentos cisco da UA, foram efectuadas configurações de forma a responder às seguintes premissas:

- ✓ Inventariação dos dispositivos existentes na rede e produção de relatórios com informação filtrada em consonância com a necessidade do momento.
- ✓ Detecção de sistemas desactualizados (Cisco IOS) e distribuição de imagens de software.
- ✓ Armazenamento das configurações implementadas nos equipamentos, registo de alterações efectuadas e distribuição em massa de configurações, sem recorrer à configuração manual (CLI) de cada equipamento.
- ✓ Monitorização de *syslogs* com notificação automática em caso de ocorrência de problemas.
- ✓ Implementação de políticas de configuração de equipamentos.

RME

Figura 25 – RME, interface Web

Durante o setup inicial do LMS, foi efectuada a descoberta da rede de forma a popular o DCR com os dispositivos encontrados e automaticamente associá-los às aplicações individuais como o RME.

Durante a instalação do RME, são criadas tarefas com calendarização própria para a inventariação por colecção e “polling”. Estes dois métodos são utilizados periodicamente pelo RME para a recolha de informação acerca dos dispositivos de rede. A inventariação por colecção recolhe os dados de todos os dispositivos e actualiza a base de dados do inventário. Por “polling”, é apenas verificado um valor específico da MIB, para a detecção de alterações do timestamp (registo de tempo), e, no caso de existir um novo timestamp, o RME sinaliza a alteração de inventário para proceder à recolha de informação e actualizar a base de dados.

Como a inventariação por “collection ” gera mais tráfego que a inventariação por “polling“, consumindo desta forma uma maior largura de banda, a periodicidade da 1ª é definida por defeito para uma vez por semana, enquanto a 2ª é de uma vez por dia (Figura 26).

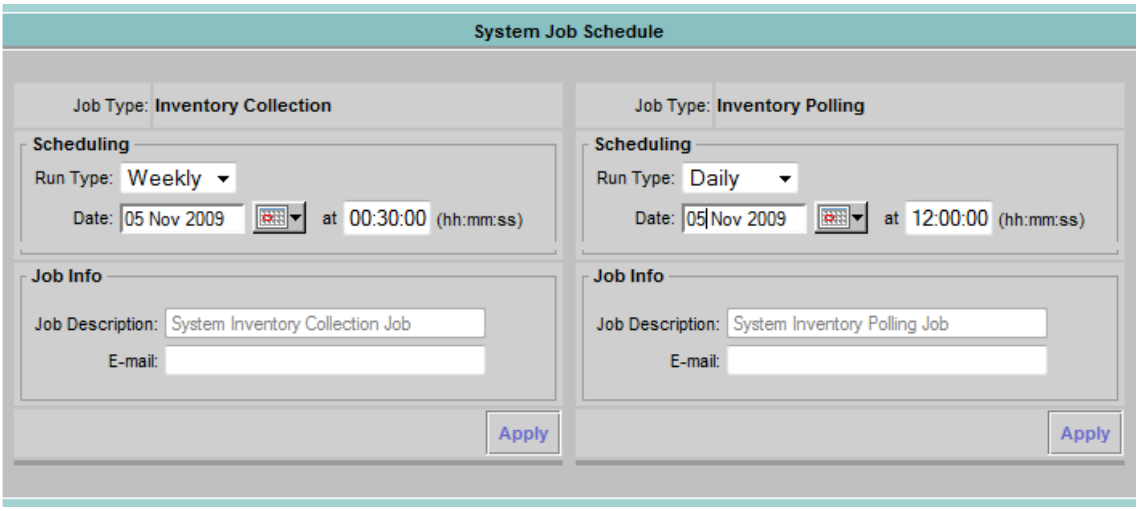


Figura 26 – RME, configuração da calendarização de tarefas

A partir do momento que os dispositivos são adicionados à base de dados do RME, este começa a receber informação à medida que as tarefas de inventariação agendadas vão sendo executadas. Com base nesta informação, o RME disponibiliza diferentes tipos de relatórios predefinidos, através de cada uma das suas aplicações internas.

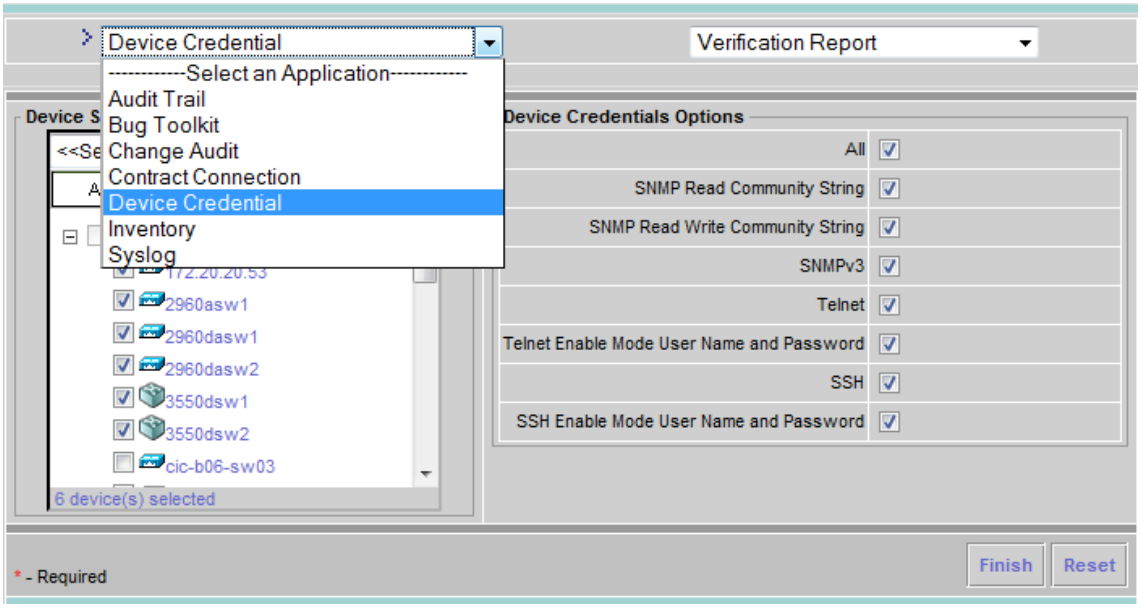


Figura 27 – RME, configuração de relatórios (1)

As aplicações disponíveis são as seguintes (Figura 27):

- **Audit Trail**: Reporta alterações efectuadas nas configurações do RME.
- **BugToolkit**: Permite a identificação e verificação do estado de erros nos dispositivos.
- **Change Audit**: Reporta alterações efectuadas na rede, incluindo configuração, inventario, software, e versão do IOS.
- **Contract Connection**: Disponibiliza informação acerca dos contratos de suporte acordados com a Cisco, de todos os dispositivos.
- **Device Credential**: Verifica as credenciais dos dispositivos e reporta estado de cada uma
- **Inventory**: Gera relatórios baseados na inventariação da informação dos dispositivos recolhida pelo RME (Figura 28)
- **Syslog**: Mostra a listagem de mensagens de syslog dos dispositivos, recebidas pelo RME

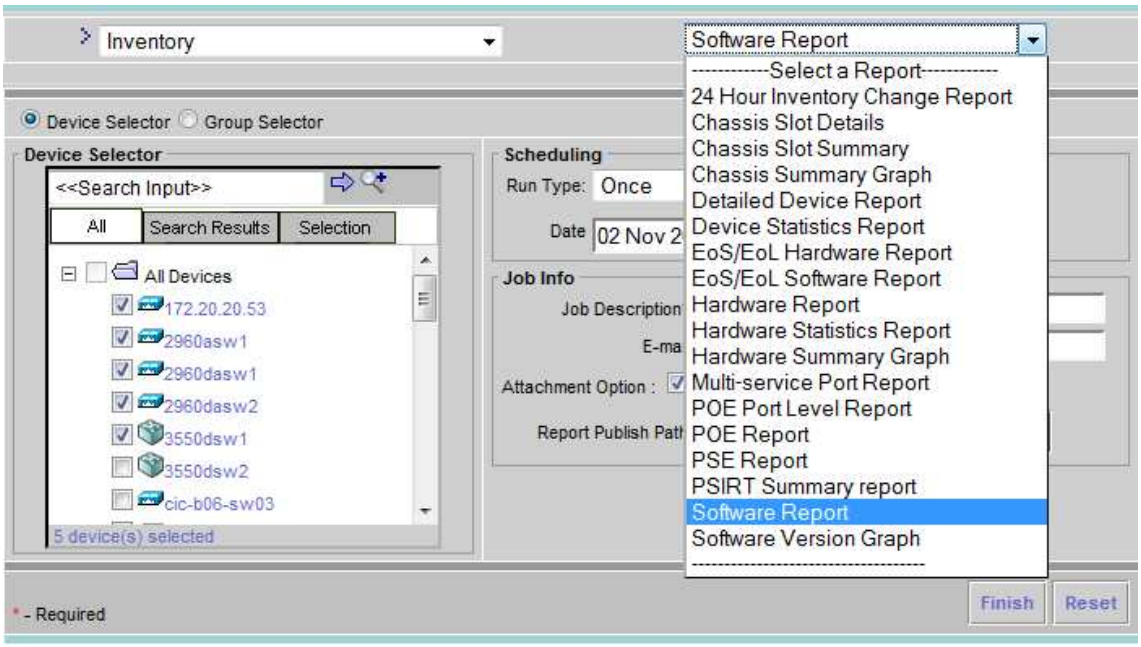


Figura 28 – RME, configuração de relatórios (2)

Os relatórios predefinidos, obedecem a um conjunto de critérios tais como, por exemplo, a listagem categorizada por tipo de equipamento gerada pelo "Software Report" (Figura 29). O RME permite também a criação de relatórios personalizados, baseados em critérios definidos através de templates, que organizam a informação a partir das variáveis pretendidas.

Category : Switches and Hubs

Cisco Catalyst 2960 Series Switches

Device Name	Updated At	System Description	Location	Contact	Serial Number	Image Version	Chassis Vendor Type	System Image File	Config Register Value
2960dasw1	Nov 17 2009 00:30:37	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(40)SE, RELEASE SOFTWARE (fc3) Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Fri 24-Aug-07 01:55 by myl			FOC1127U120	12.2(40)SE	cevChassisCat2960G24	flash:/c2960-lanbasek9-mz.122-40.SE.bin	0xf
2960asw1	Nov 17 2009 00:30:35	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(40)SE, RELEASE SOFTWARE (fc3) Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Fri 24-Aug-07 01:55 by myl			FOC1033Z2VP	12.2(40)SE	cevChassisCat296024TT	flash:/c2960-lanbasek9-mz.122-40.SE.bin	0xf

Cisco Catalyst 3550 Series Switches

Device Name	Updated At	System Description	Location	Contact	Serial Number	Image Version	Chassis Vendor Type	System Image File	Config Register Value
3550dsw2	Nov 20 2009 12:00:46	Cisco IOS Software, C3550 Software (C3550-IPSERVICESK9-M), Version 12.2(40)SE, RELEASE SOFTWARE (fc3) Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Fri 24-Aug-07 02:15 by myl			CAT0617X0GQ	12.2(40)SE	cat355024	flash:/c3550-ipservicesk9-mz.122-40.SE.bin	0x10f
3550dsw1	Nov 20 2009 12:00:46	Cisco IOS Software, C3550 Software (C3550-IPSERVICESK9-M), Version 12.2(40)SE, RELEASE SOFTWARE (fc3) Copyright (c) 1986-2007 by Cisco Systems, Inc. Compiled Fri 24-Aug-07 02:15 by myl			CAT0730X0K5	12.2(40)SE	cat355024	flash:/c3550-ipservicesk9-mz.122-40.SE.bin	0x10f

Figura 29 – RME, exemplo de relatório

A gestão das imagens de software disponibilizada pelo RME, permite uma análise prévia dos sistemas em execução nos dispositivos e a realização de "upgrades" automaticamente. Para testar a funcionalidade, foi efectuada a sequência de acções:

- ✓ Análise dos dispositivos para avaliação de recursos necessários à implementação do novo software. O RME fornece recomendações para o upgrade através da comparação do sistema em execução com a imagem escolhida. Para isto, dispõe de uma funcionalidade que permite a ligação à base de dados de imagens de software da Cisco Systems, e a visualização das versões existentes até à data para um dispositivo em particular.

- ✓ Adição das imagens de software pretendidas ao repositório local, utilizando a função que permite o download imediato ou agendado, a partir do repositório online da Cisco.

- ✓ Criação tarefas para a distribuição de imagens de software pelos dispositivos. Esta funcionalidade dispõe de quatro métodos de distribuição:
  - o Básico: permite a selecção de dispositivos nos quais é pretendida a implementação de uma nova imagem. A imagem corrente é verificada para a recomendação da melhor imagem para distribuição.
  - o Avançado: A diferença da anterior é a possibilidade de escolher uma imagem que não se encontre no repositório do LMS, indicando a sua localização. A imagem indicada é validada e verificada relativamente a dependência e requisitos.
  - o Por imagem (Figura 30): permite a selecção de uma imagem armazenada no repositório, para implementação em dispositivos suportados

- Fonte remota: Permite a selecção de uma imagem, que irá ser guardada temporariamente num dispositivo, para que este sirva de fonte de distribuição para os dispositivos suportados.

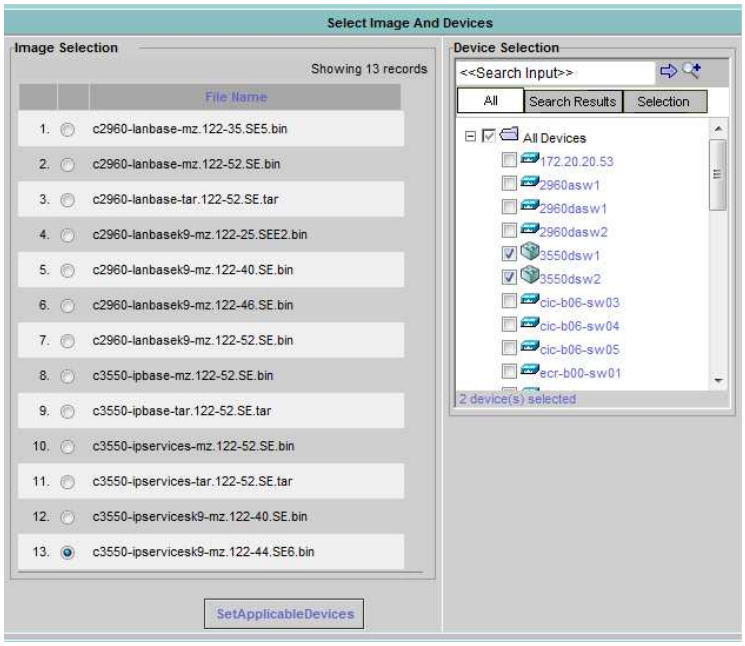


Figura 30 – RME, método de distribuição de imagens

Device Center

O Device Center é um portal, que centraliza as funções de diagnóstico para um determinado dispositivo. Permite a partir de um ponto central, o lançamento de ferramentas que facilitam a resolução de problemas e a visualização de um sumário de informações que possibilitam uma análise rápida (Figura 31)

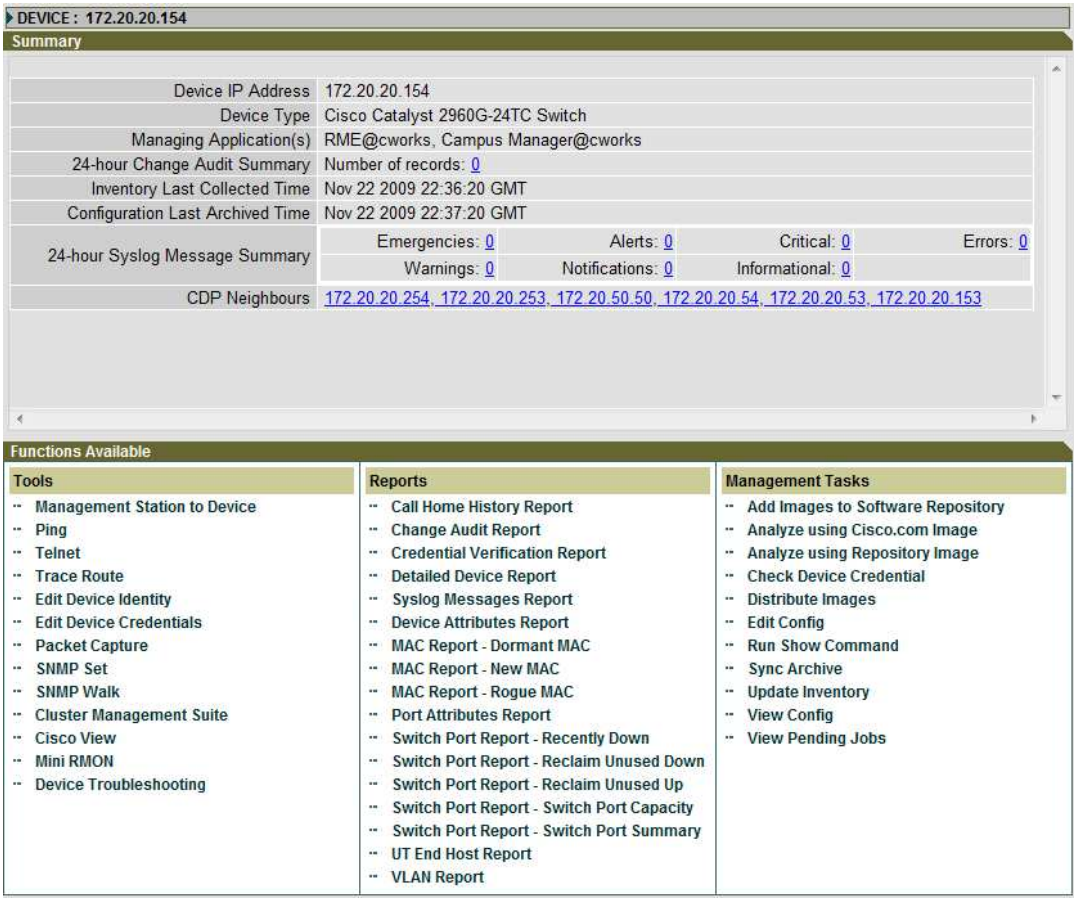


Figura 31 – Device Center

O diagnóstico de um disposivo pode ser realizado a partir do lançamento de procedimentos seguidamente descritos:

- Visualização de relatórios diários (24-hour reports)
- Teste de conectividade através da ferramenta basada no protocolo Ping
- Lançamento da ferramenta para verificação de credenciais
- Relatório detalhado do dispositivo, que permite a visualização de informações relativas a memória disponível, imagem e configuração IP.
- No caso de serem detectadas falhas, é possível o lançamento da aplicação Cisco View para a execução de alterações em interfaces ou portas.
- No caso de o dispositivo ser um switch, é disponibilizado um relatório relativo a utilização de portas.

Cisco View

O Cisco View é uma ferramenta especificamente direccionada à configuração de elementos. Permite uma visualização gráfica dos dispositivos e disponibiliza funções para configuração

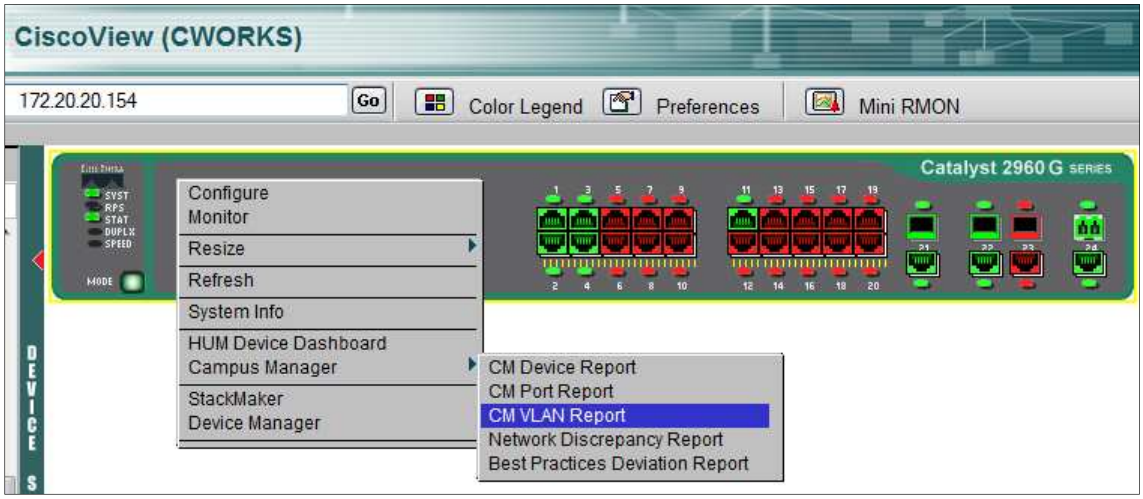


Figura 32 –Cisco View, visualização de chassis

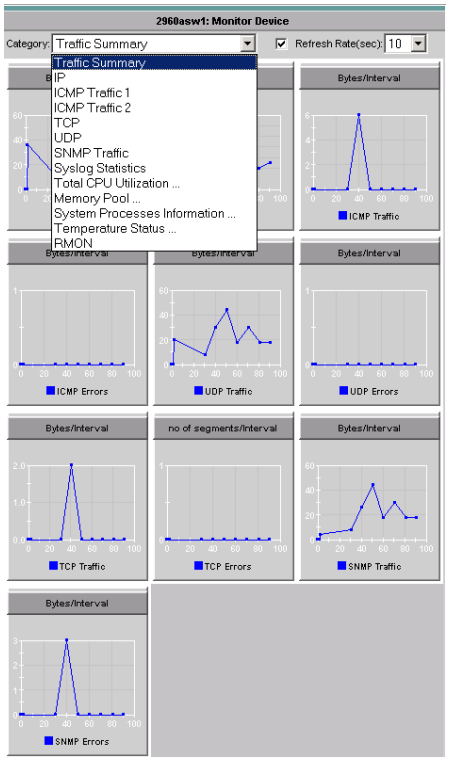


Figura 33 – Mini RMON, estatísticas de trafego

4.2.1.4 Gestão de rede

Um dos aspectos importantes a ter em conta para o diagnóstico de problemas de rede, à medida que estes aparecem, é o conhecimento associado à percepção real de como todos os elementos estão fisicamente e logicamente conectados na rede. O Campus Manager é a aplicação do LMS que fornece a gestão de conectividade em ambiente gráfico, permitindo a visualização e configuração das ligações físicas e lógicas, verificação da spanning tree, e o tratamento de discrepâncias de configuração existentes na rede.

Os objectivos traçados para a implementação do Campus Manager foram os seguintes:

- Auto-descoberta e visualização da topologia de rede
- Configuração de protocolos (VLANs e Spanning Tree) e diagnóstico de problemas da 2ª camada de rede,
- Detecção de utilizadores e estações de trabalho na rede, e identificação das portas dos *switches* a que estão conectados.

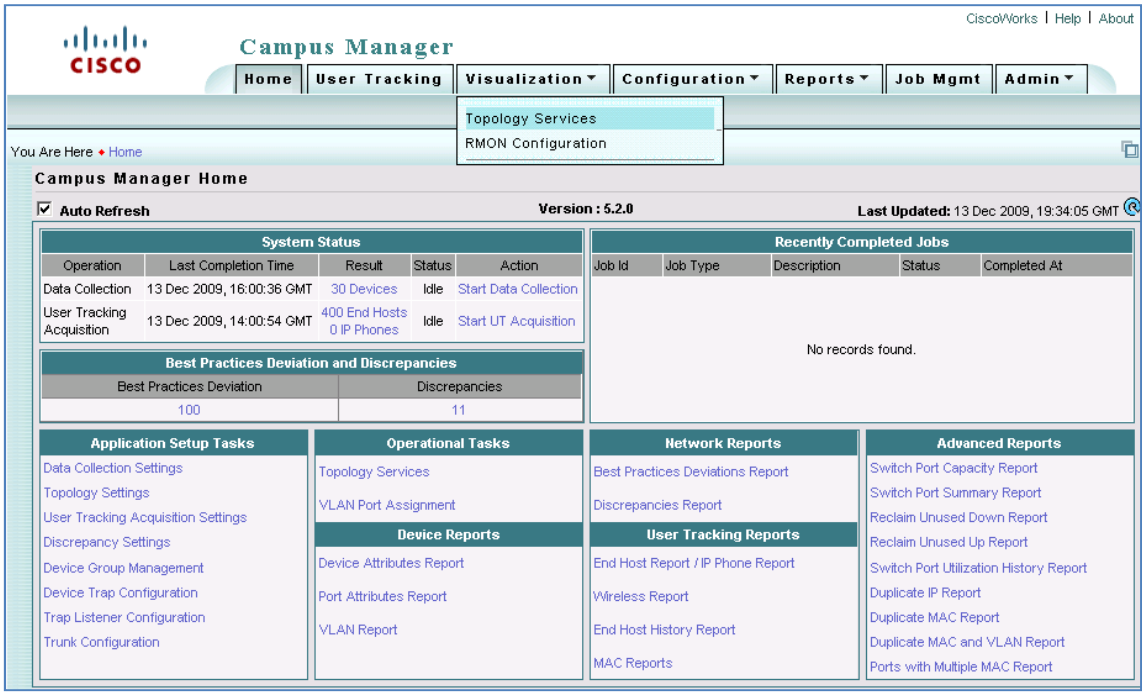


Figura 34 - Painel de navegação do CW Campus Manager

Durante o processo inicial de descoberta da rede efectuado pelo *Common Services*, são construídos os mapas de conectividade física da rede a partir das tabelas de vizinhança CDP colectadas por SNMP. Em paralelo, o Campus Manager recolhe informação adicional relativa a interfaces, portas, protocolo *Spanning Tree*, domínios VTP, configuração de VLANs, etc. Esta informação é catalogada, armazenada, actualizada, em intervalos de tempo regulares, e visualizável através dos diversos relatórios disponibilizados pelo CM.

Após a recolha de dados dos equipamentos de rede, é possível recorrendo à funcionalidade Topology Services visualizar os mapas de topologia e a informação associada. A aplicação *Topology Services* utiliza um interface que é lançado pela tecnologia "Java Web Start", sendo necessária a instalação prévia na máquina cliente de um JRE específico, fornecido pelo Campus Manager na 1ª vez que a aplicação é lançada.

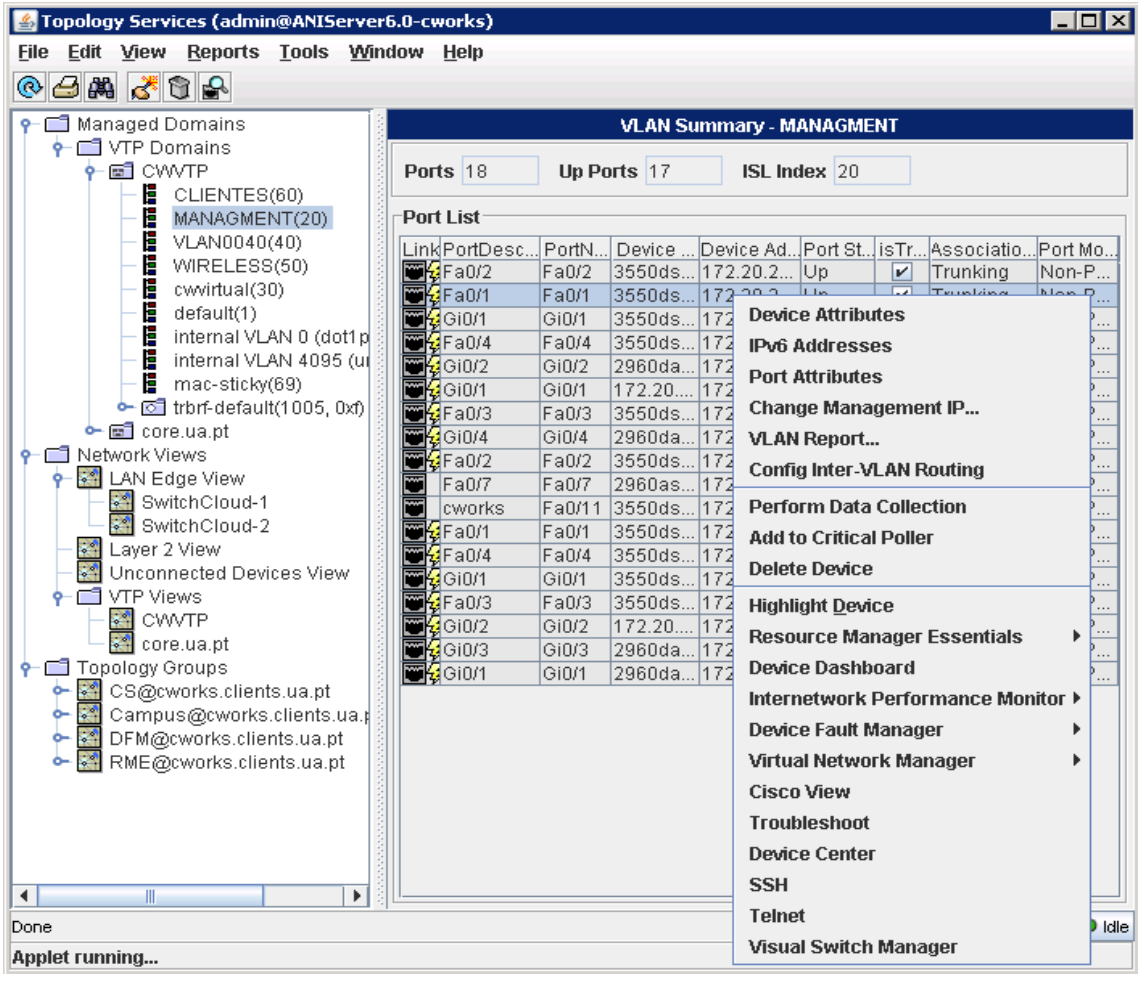


Figura 35 – Campus Manager Topology Services

A janela principal da aplicação *Topology Services* (Figura 35), é constituída por um painel de navegação em árvore e um painel com o sumário dos dispositivos em formato tabular. O painel de navegação encontra-se organizado em três directórios que contêm os diversos tipos de visualizações:

- *Managed Domains*: Contém visualizações para domínios VTP e ATM. As visualizações de VTP permitem a gestão de VLANs.
- *Network Views*: Contém visualizações globais predefinidas, que possibilitam a visualização de dispositivos de segunda e terceira camada de rede, dispositivos descobertos cuja informação de conectividade é desconhecida e dispositivos associados a um domínio VTP.
- *Topology Groups*: Contem grupos predefinidos e personalizados de visualização de dispositivos.

O resultado da descoberta da conectividade física, é facilmente visualizável através dos mapas que topologia de rede disponibilizados. De seguida são descritos alguns exemplos de mapas possíveis de gerar a partir do directório *Network Views:*

- **LAN Edge View:** Mostra a conectividade de rede entre dispositivos de 3º nível (*layer 3*).
- **Switch Cloud View:** Mostra a os dispositivos de 2º nível (*layer 2*) que se encontram entre 2 dispositivos de 3º nível (Figura 36)

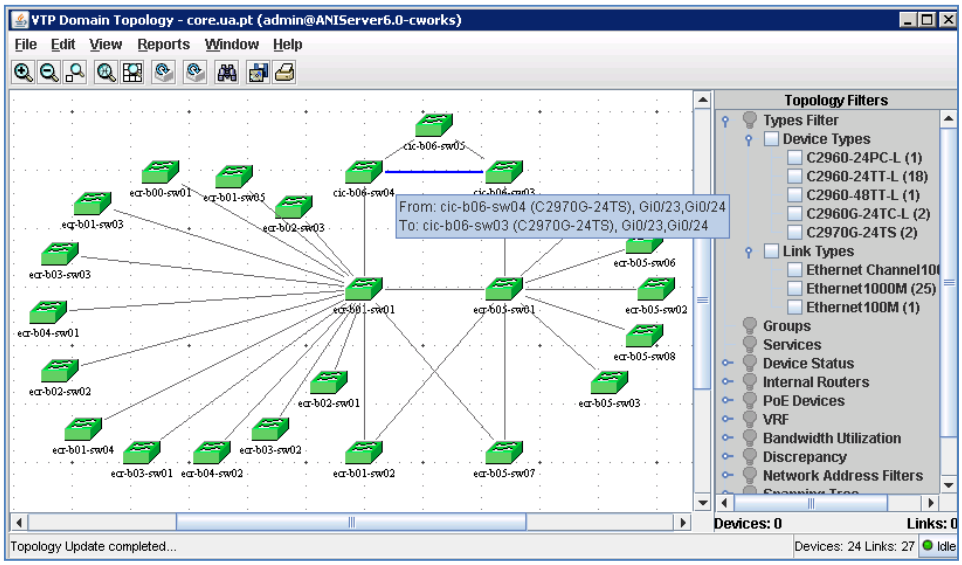


Figura 36 – Mapa de topologia de rede (UA)

- **Layer 2 View:** Mostra a informação acerca da 2ª camada de rede, relativa a switches LAN e ATM, routers, dispositivos MLS, hubs e switch-probes.
- **Unconnected Devices View:** Mostra os dispositivos cuja informação de conectividade não pôde ser obtida, incluindo os dispositivos não suportados pelo topology services.
- **VTP Views:** Mostra os dispositivos pertencentes a um domínio VTP (Figura 37).

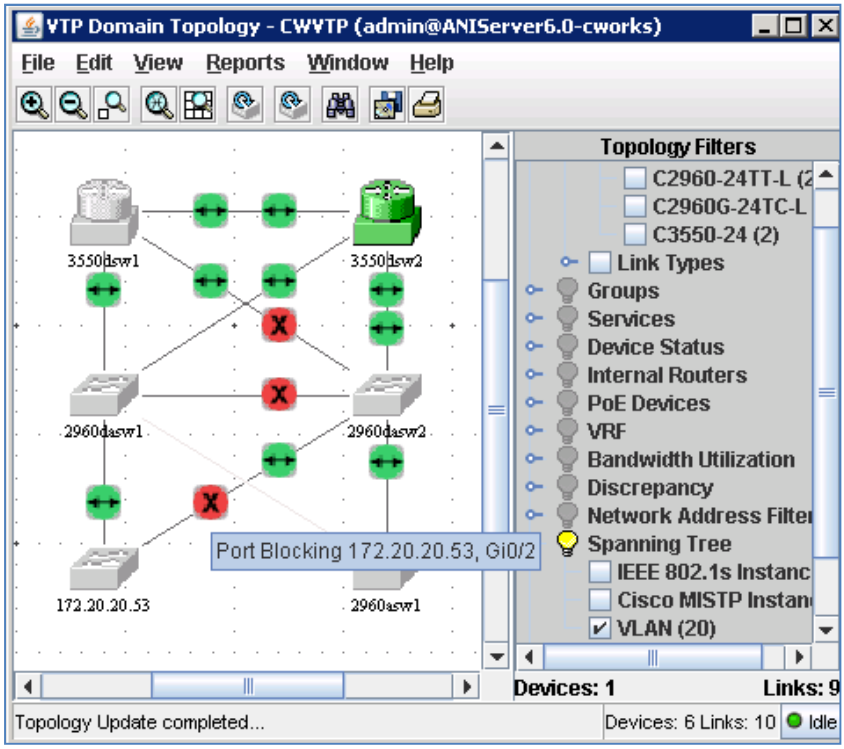


Figura 37 - Mapa de topologia de rede (Lab.)

No mapa da Figura 37, também encontra-se representada a configuração do protocolo spanning tree. O Campus Manager disponibiliza funcionalidades avançadas para a gestão deste protocolo, tais como: Per VLAN Spanning Tree (PVST), Protocol, Multiple Spanning Tree Protocol (MSTP), and Multi-Instance Spanning Tree Protocol (MISTP).

A partir dos mapas de topologia também é possível o lançamento directo de diversos relatórios do Campus Manager, que variam dependendo do tipo de mapa. Por exemplo, a partir do mapa de topologia de segunda camada de rede é possível a visualização dos seguintes relatórios:

- Best Practices Deviations Report
- Device Attributes Report
- Discrepancies Report
- Port Attributes Report
- VLAN Report

Outro aspecto a salientar é o facto de ser possível realizar inúmeras configurações de rede através do interface gráfico, o que torna o processo bastante mais fácil, em relação á edição manual por CLI.

N-Hop View

O portlet N-Hop View é uma funcionalidade Integrada no CiscoWorks Portal que permite a visualização de uma parte da rede, definida por nº de hops partir de um dispositivo raiz. Este mapa é actualizado de uma muito mais rápida que os mapas regulares do *Topology services* e suporta até 30 dispositivos. Adicionalmente também permite a visualização de alertas do DFM e o acesso a um conjunto de aplicações por dispositivo (Figura 38).

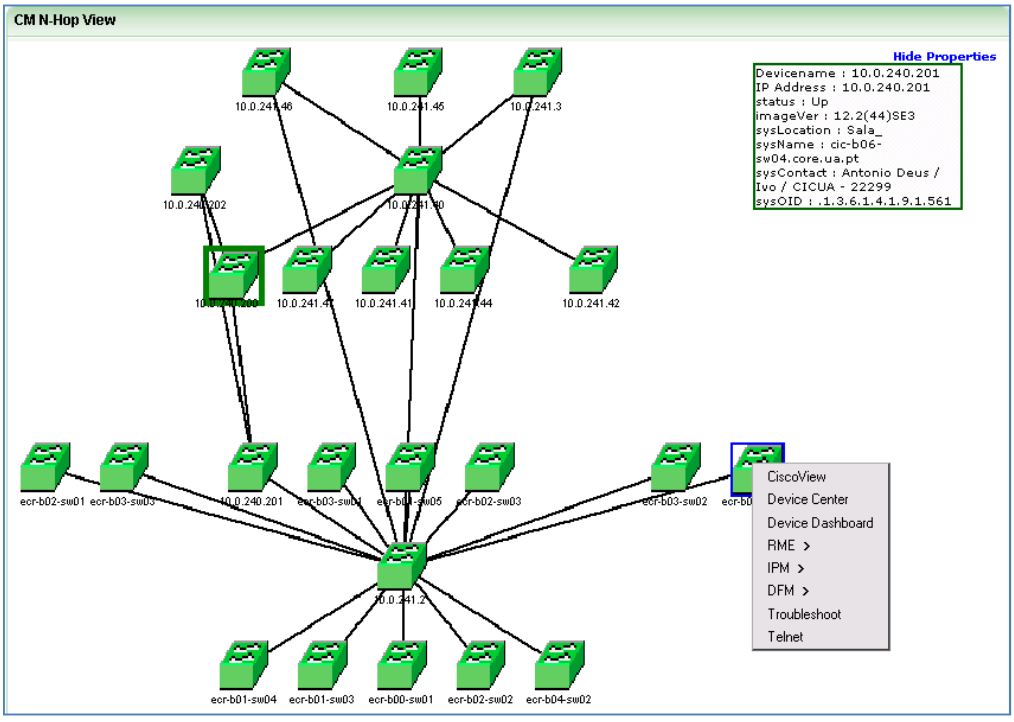


Figura 38 – Campus Manager N-Hop View

4.2.1.5 Gestão de falhas

O CiscoWorks LMS fornece um sistema para Gestão de Falhas, acerca do qual foi de maior interesse testar as funcionalidades que providenciam soluções para os seguintes pontos:

- Detecção, isolamento e correcção de falhas na rede
- Monitorização da conectividade e potenciais problemas das interfaces
- Conhecimento da robustez dos equipamentos e rede
- Resolução de problemas antes que a degradação da rede afecte os seus utilizadores
- Minimização de tempo sem conectividade e degradação de serviço

Device fault manager

O DFM monitoriza proactivamente indicadores de falhas na rede e nos equipamentos, permitindo um diagnóstico preciso de problemas. A determinação de variáveis e eventos que caracterizam a operatividade de um dispositivo é efectuada de forma autónoma, pelo que a intervenção humana é dispensada para o efeito, o que proporciona uma eficiente gestão de falhas.

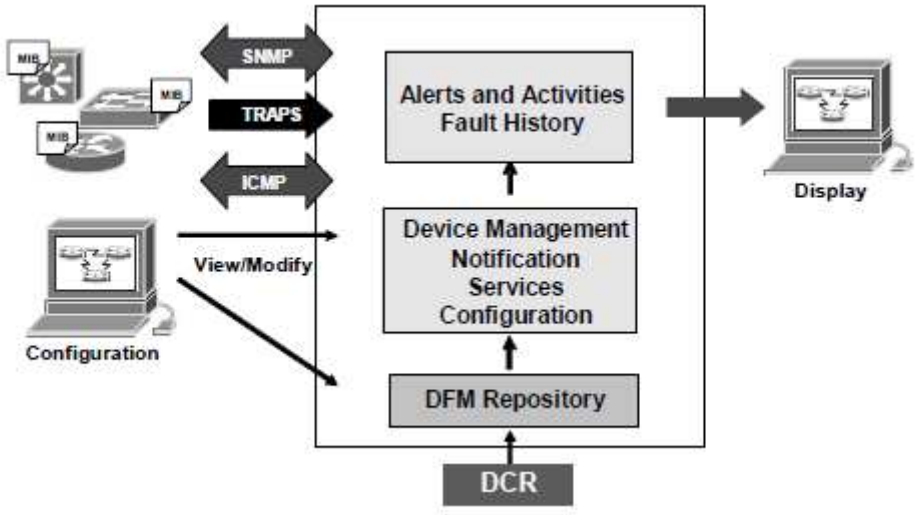


Figura 39 – Arquitectura do DFM

Os métodos utilizados pelo DFM para a descoberta e disponibilização em tempo real de informação de falhas são pooling SNMP e traps SNMP (Figura 39). A primeira tarefa realizada foi a importação manual de dispositivos a partir do DCR de modo a serem geridos pelo DFM. Após este processo, foram efectuadas configurações para monitorização de alertas e actividades nos dispositivos

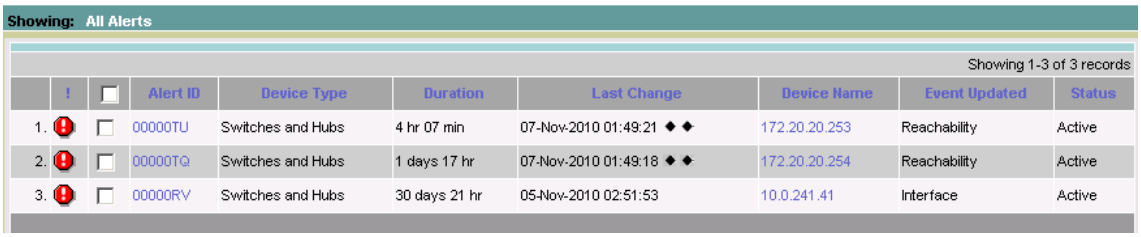


Figura 40 – DFM, visualização de alertas

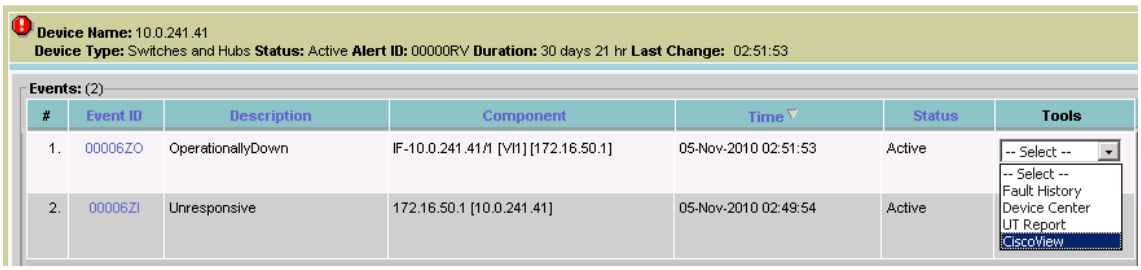


Figura 41 – DFM, visualização detalhada de um alerta

A visualização de alertas (Figura 40) e actividades requer um constante contacto visual com o interface de monitorização. Para aliviar a esta necessidade o DFM disponibiliza serviços de notificação tais como, correio electrónico, Traps SMNP e mensagens de Syslog. Cada um destes mecanismos providencia um sumário de alertas ou eventos.

4.2.1.6 Gestão de desempenho

O isolamento de problemas de desempenho, localização de pontos de estrangulamento, medição de latência e a realização de diagnósticos e análises de tendências em redes multi-protocolares, são alguns dos desafios enfrentados na gestão de redes.

IPM

O primeiro passo a dar na configuração da gestão de desempenho do IPM, é a criação de colectores. Os colectores são os responsáveis pela recolha de dados, e são constituídos por quatro componentes:

- Dispositivo fonte: Ponto a partir do qual o IPM faz medições de latência e disponibilidade. O IPM configura o protocolo *Cisco IOS IP SLA* no dispositivo, por SNMP

- Dispositivo destino: Destino da fonte de operações (medições IP SLA), do qual os dados da resposta devem ser recolhidos. Um destino pode ser um host, ou outro dispositivo que suporte *Cisco IOS IP SLA* (responder).

- Operações de teste: As operações de teste de tráfego, simulam tráfego real, para um protocolo específico. Por exemplo, para medir a latência de uma sessão VoIP, uma operação de teste UDP é criada, e definida para enviar uma série de pacotes UDP de 60 bytes, com um tipo específico de serviço (ToS), valor, e número da porta de destino

- Calendarização da recolha de dados: Um colector pode ser programado para ser executado em qualquer altura, ou continuamente durante intervalos de tempo. Este agendamento flexível, torna os *IP SLAs* adequados, quer para monitorização do nível de serviço, quer para a realização de diagnósticos.

IPM Availability Dashboard

Operation Types	No. of Collectors	Availability %				
		0-50	51-90	91-95	96-98	99-100
Echo	3	0	0	0	0	3
TCPConnect	2	2	0	0	0	0
DNS	2	0	0	0	0	2
UDPEcho	1	0	0	0	0	1
PathEcho	1	0	0	0	0	1

IPM Highest Latency

Collector Name	Operation Type	Latency
IPM-dws1_2960asw1_ipm-dns	DNS	4(ms)
dns-dsw1_cworks.testes.lms_ipm-dns	DNS	3(ms)
IPM-dws1_2960asw1_DefaultUDPEcho	UDPEcho	2(ms)
IPM-dws1_2960asw1_DefaultIpEchoPri3	Echo	1(ms)
IPM-dws1_2960asw1_DefaultNNTP	TCPConnect	0(ms)

Figura 42 – IPM, estatísticas de disponibilidade e latência

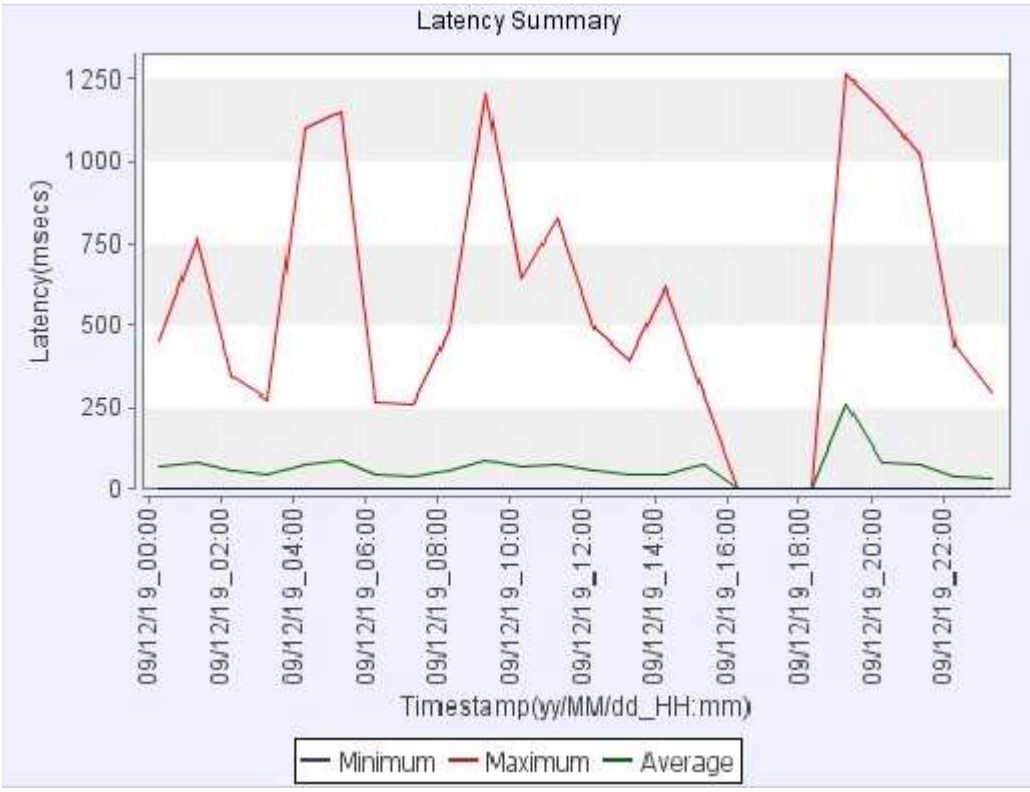


Figura 43 – IPM, Gráfico de latência

Health and Utilization Monitor

O CiscoWorks HUM, como já foi referido, monitoriza parâmetros de desempenho de equipamentos Cisco, relativos a: utilização de processador, utilização memória, disponibilidade de interfaces, disponibilidade dispositivos, entre outros. Esta ferramenta integra-se na gestão de desempenho da rede, sendo direccionada à monitorização dos componentes dos dispositivos. Esta monitorização é efectuada consultando os dispositivos através de SNMP.

As Figuras 44,45 e 46 exemplificam algumas das estatísticas que o HUM disponibiliza.

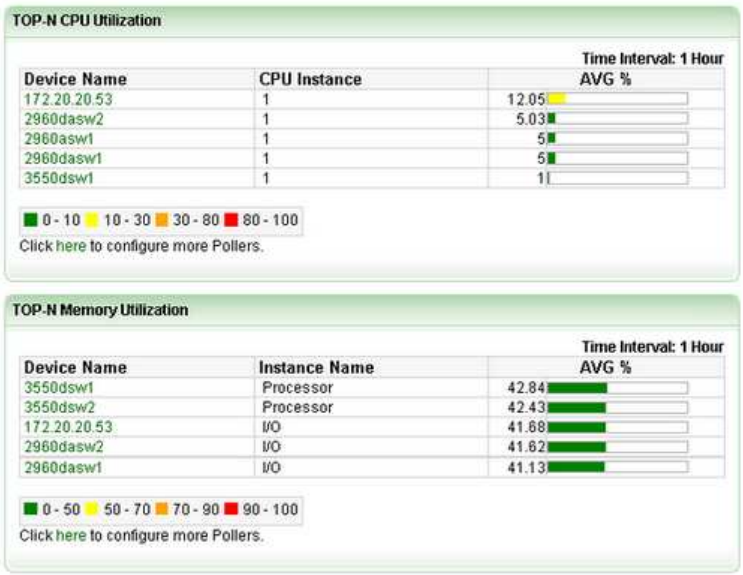


Figura 44 – HUM, estatísticas TOP-N

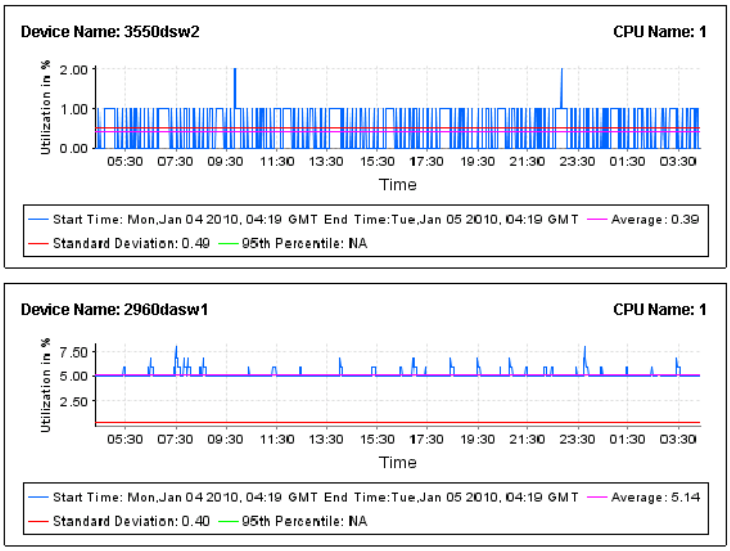


Figura 45 – HUM, gráficos de utilização de CPU

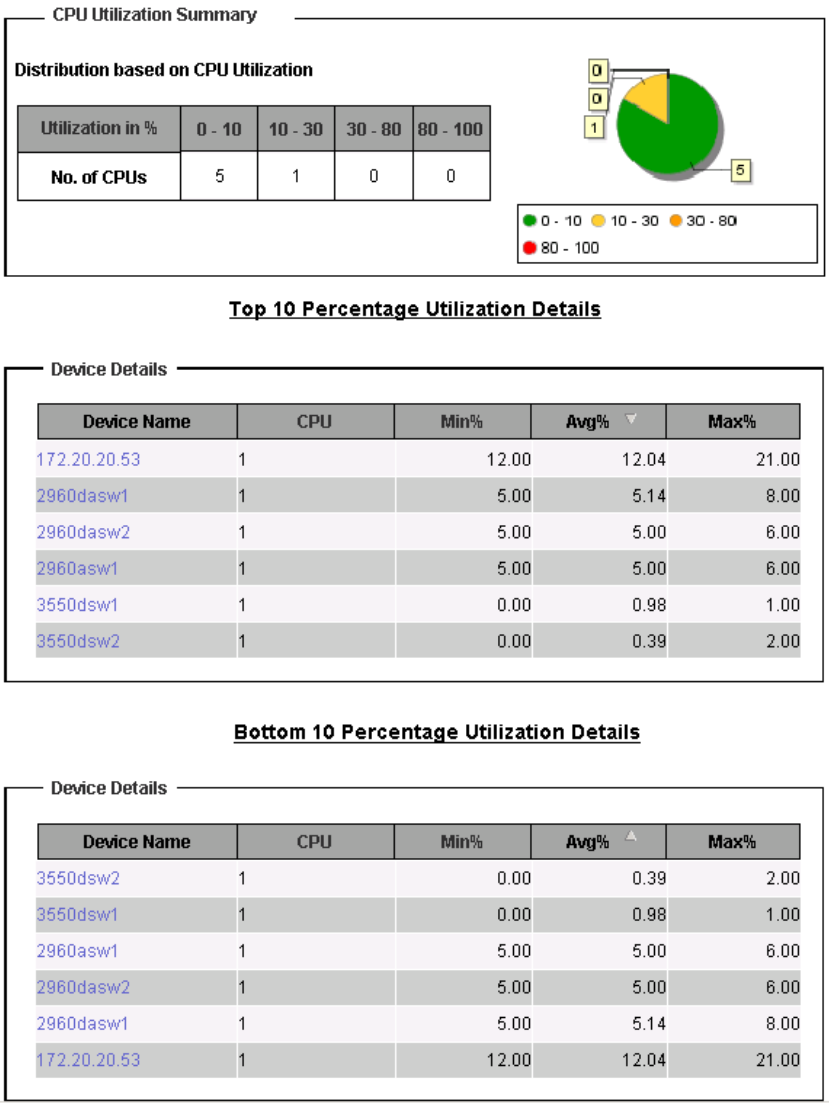


Figura 46 – HUM, relatório de utilização de CPU.

4.2.2 Cacti

A aplicação Cacti requer a configuração de vários utilitários para que funcionem em conjunto de forma a possibilitar a apresentação da informação no Interface Web que disponibiliza. Nestes utilitários estão incluídos um servidor web, uma base e dados, PHP e RRD Tool. Todos os trabalhos de instalação e configuração do servidor e plugins complementares, foram efectuados seguindo as indicações apresentadas nos manuais e documentação adicional existente.

Os requisitos para os dispositivos de rede que se pretendem monitorizar com o Cacti, passam basicamente pela activação e configuração das credenciais SNMP nos mesmos. De um modo geral qualquer dispositivo que suporte SNMP é elegível para ser monitorizado pelo Cacti. Estas configurações já haviam sido efectuadas durante a montagem do cenário, pelo que se passou directamente para a configuração do Cacti.

O primeiro passo para a criação de gráficos é a adição ou selecção de um dispositivo (agente SNMP). Os métodos para adição de dispositivos são simples e podem ser efectuados de forma manual ou automatizada pela definição de templates para descoberta de rede. A Figura 47 mostra um exemplo de definição de um dispositivo.

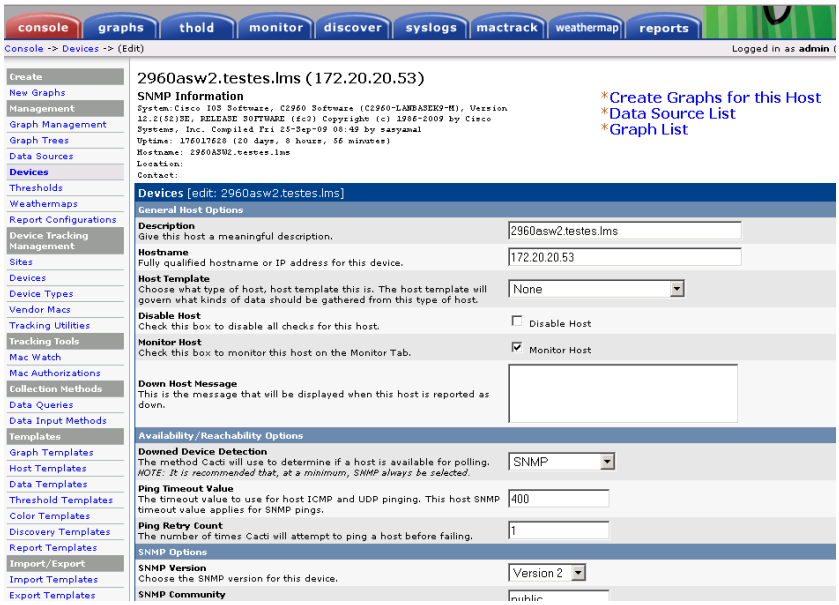


Figura 47 – Cacti, adição de dispositivos

A definição de dispositivos requer a especificação de detalhes importantes, tais como o tipo e nome do *"host"* na rede, e parâmetros SNMP

Após a criação do de um dispositivo é possível escolher os *"Graph templates"* e "D*ata Queries"* associados, para dar inicio à recolha de informações e criação de gráficos (Figura 48)

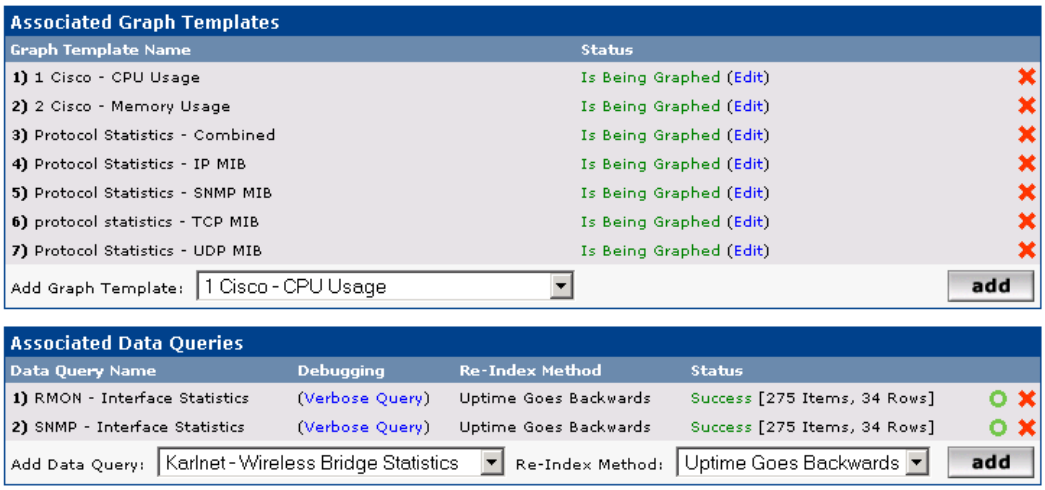


Figura 48 – Cacti

O Cacti é provido de funcionalidades avançadas para personalização de templates associados à caracterização e recolha de informação dos equipamentos geridos. Neste trabalho foram testados diversos templates de origem e adicionados posteriormente. Na matéria de monitorização de tráfegos, destacam-se aqui os seguintes templates:

- SNMP Interfaces Statistics - Fornece estatisticas de trafego obtidas por SNMP. Todos os scripts e templates associados a esta *querie* fazem parte do pacote distribuído do Cacti.

- RMON Interfaces Statistics – Fornece estatísticas de rede recorrendo à extensão da MIB2, RMON. Todos os scripts e templates associados a esta *querie* não fazem parte do pacote original, pelo que tiveram que ser editados e importados (Figura 49) para o Cacti.

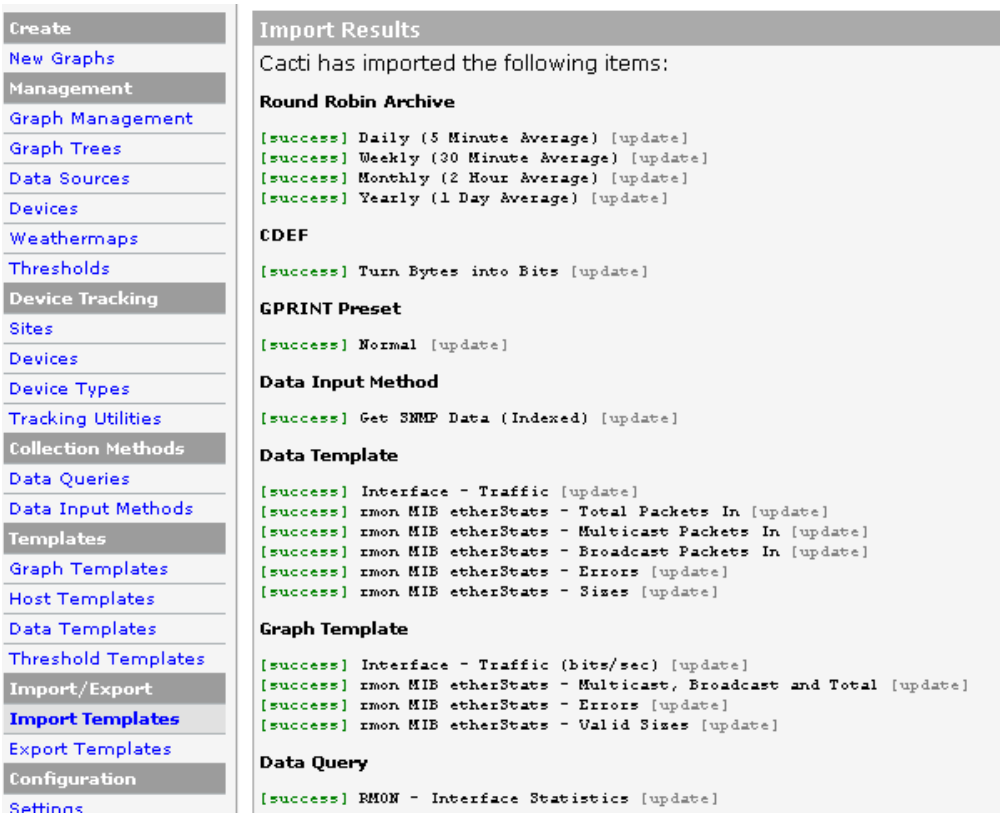


Figura 49 – Cacti, exemplo de importação de template.

O passo seguinte, para finalizar a criação de gráficos, é a escolha de portas que se pretendem monitorizar (Figura 50). Esta informação é obtida pela realização automática do comando *snmpwalk* (para o caso apresentado).

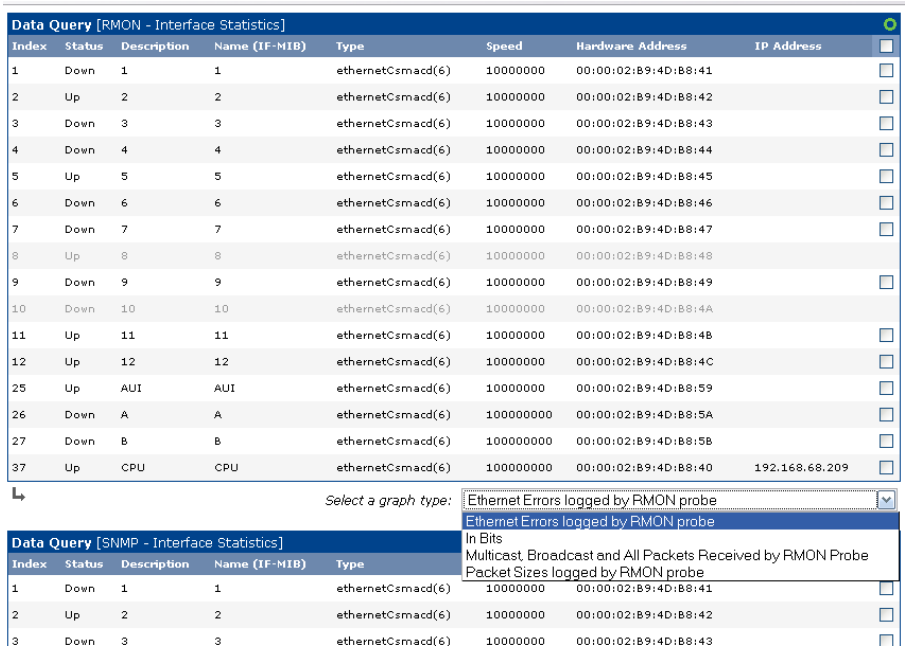


Figura 50 - Cacti, RMON – Interface Statistics

A Figura 51 apresenta um exemplo de monitorização de tráfego em ambiente real, num equipamento de rede Cisco em produção na Universidade de Aveiro.

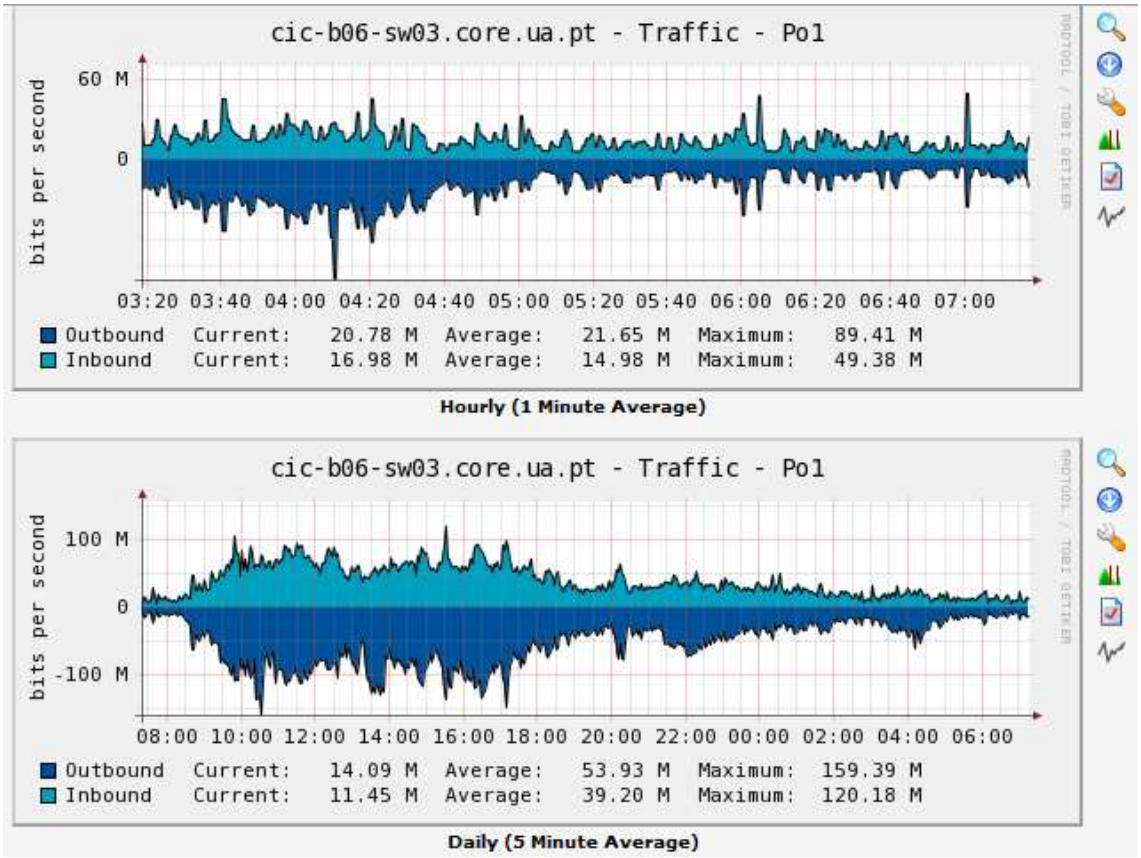


Figura 51 – Cacti, Monitorização de tráfego em ambiente real.

Existem diversos *plugins* que podem completar o desempenho do Cacti na monitorização de uma rede. Neste trabalho foram instalados e testados com sucesso alguns, que representam a complementaridade da gestão de desempenho nativa do cacti, com as restantes áreas funcionais do modelo FCAPS. Exemplos disto são os plugins: *treshold, monitor, MacTrack, discover, syslogs, weathermaps, e reports*.

4.2.3 NTOP

A instalação e configuração do NTOP foram efectuadas seguindo indicações descritas na documentação disponível na Web para o sistema operativo Ubuntu (https://help.ubuntu.com/community/Ntop). Estas tarefas são processos simples, e foram realizadas de forma a se proceder à captura de tráfego através da tecnologia port mirroring (SPAN, em termos da Cisco), configurada num dos equipamentos utilizados (Figura 21).

Com o NTOP foi possível visualizar a utilização corrente da rede, a listagem de *hosts* existentes e relatórios referentes a informação relativa a tráfego IP gerado por cada *host*. De seguida são mostrados alguns exemplos de Informação registada pelo NTOP para cada host:

- DATA Sent /received – tráfego total gerado e recebido por cada host, classificado de acordo com o protocolo de rede (IP, IPX, AppleTalk, etc.) e com o protocolo IP (FTP, HTTP, NFS,etc.).

Network Traffic [All Protocols]: All Hosts - Data Sent+Received

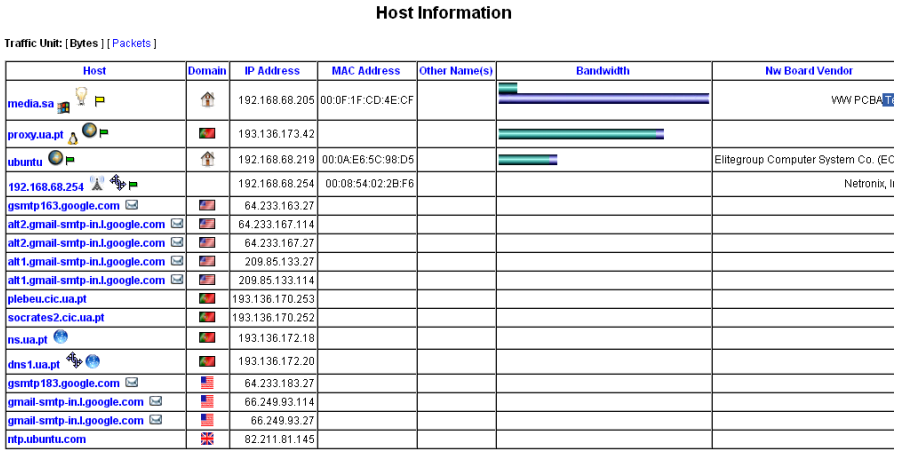
Hosts: [All] [Local Only] [Remote Only] Data: [All] [Sent Only] [Received Only]

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP	AppleTalk	NetBios	OSI	IPv6	STP	IPSEC	OSPF	IGM
media.sa		90.4 MB	49.8 %	89.6 MB	759.4 KB	2.6 KB	0	0	0	0	17.1 KB	0	0	0	0	0	0	0	12
proxy.ua.pt		66.7 MB	36.7 %	66.7 MB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
ubuntu		23.7 MB	13.1 %	22.8 MB	878.3 KB	2.2 KB	0	0	0	0	44.5 KB	0	0	0	0	0	0	0	
dns1.ua.pt		463.4 KB	0.2 %	0	463.4 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
192.168.68.254		87.4 KB	0.0 %	0	35.1 KB	3.2 KB	0	0	0	0	49.2 KB	0	0	0	0	0	0	0	
ns.ua.pt		45.2 KB	0.0 %	0	45.2 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
gmail-smtp-in.l.google.com		40.0 KB	0.0 %	40.0 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
gmail-smtp-in.l.google.com		39.7 KB	0.0 %	39.7 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
alt1.gmail-smtp-in.l.google.com		34.2 KB	0.0 %	34.2 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
alt2.gmail-smtp-in.l.google.com		32.4 KB	0.0 %	32.4 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
alt2.gmail-smtp-in.l.google.com		31.9 KB	0.0 %	31.9 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
plebeu.cic.ua.pt		29.7 KB	0.0 %	558	27.4 KB	1.7 KB	0	0	0	0	0	0	0	0	0	0	0	0	
gsmtp183.google.com		26.5 KB	0.0 %	26.5 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
socrates2.cic.ua.pt		22.6 KB	0.0 %	0	22.6 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
alt1.gmail-smtp-in.l.google.com		21.7 KB	0.0 %	21.7 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
gsmtp163.google.com		20.4 KB	0.0 %	20.4 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	0	

Note: These counters do not include broadcasts and will not equal the 'Global Protocol Distribution'

Figura 52 – NTOP – NetWork Traffic

- USED BANDWIDTH – Utilização actual, média e de pico da largura de banda.



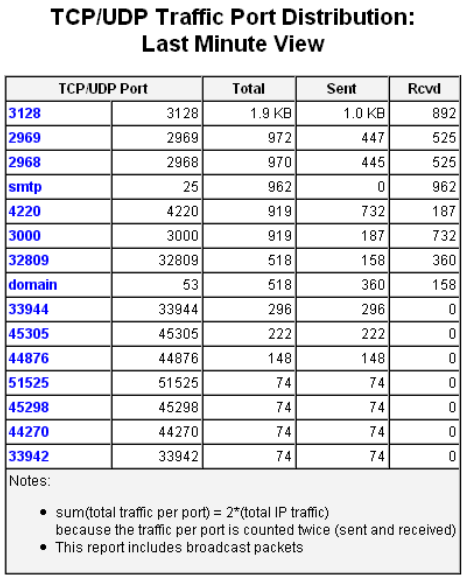
Host Information

Traffic Unit: [Bytes] [Packets]

Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth	Nw Board Vendor
media.sa		192.168.68.205	00:0F:1F:CD:4E:CF			WW PCBA
proxy.ua.pt		193.136.173.42				
ubuntu		192.168.68.219	00:0A:E6:5C:98:D5			Elitegroup Computer System Co. (EC
192.168.68.254		192.168.68.254	00:08:54:02:2B:F6			Netronix, I
gsmtp163.google.com		64.233.163.27				
alt2.gmail-smtp-in.l.google.com		64.233.167.114				
alt2.gmail-smtp-in.l.google.com		64.233.167.27				
alt1.gmail-smtp-in.l.google.com		209.85.133.27				
alt1.gmail-smtp-in.l.google.com		209.85.133.114				
plebeu.cic.ua.pt		193.136.170.253				
socrates2.cic.ua.pt		193.136.170.252				
ns.ua.pt		193.136.172.18				
dns1.ua.pt		193.136.172.20				
gsmtp183.google.com		64.233.183.27				
gmail-smtp-in.l.google.com		66.249.93.114				
gmail-smtp-in.l.google.com		66.249.93.27				
ntp.ubuntu.com		82.211.81.145				

Figura 53 – NTOP – Host Information

- IP MULTICAST – Totalidade do tráfego multicast gerado ou recebido pelo host;
- TCP SESSIONS HISTORY – Sessões TCP activas estabelecidas ou aceites pelo host e estatísticas de tráfego associadas;
- UDP TRAFFIC – Quantidade total de tráfego UDP distribuído por porta.



TCP/UDP Traffic Port Distribution: Last Minute View

TCP/UDP Port		Total	Sent	Rcvd
3128	3128	1.9 KB	1.0 KB	892
2969	2969	972	447	525
2968	2968	970	445	525
smtp	25	962	0	962
4220	4220	919	732	187
3000	3000	919	187	732
32809	32809	518	158	360
domain	53	518	360	158
33944	33944	296	296	0
45305	45305	222	222	0
44876	44876	148	148	0
51525	51525	74	74	0
45298	45298	74	74	0
44270	44270	74	74	0
33942	33942	74	74	0

Notes:

- sum(total traffic per port) = 2*(total IP traffic) because the traffic per port is counted twice (sent and received)
- This report includes broadcast packets

Figura 54 - NTOP – TCP/UDP traffic port distribution

- TCP/UDP USED SERVICES – Lista de serviços baseados no protocolo IP (e.g. portos abertos e activos) disponibilizados pelo host com uma lista dos últimos cinco hosts que os usaram;

- TRAFFIC DISTRIBUTION – Tráfego local dirigido a hosts remotos, tráfego remoto dirigido a hosts locais (os hosts locais estão ligados à rede "*broadcast*");
- IP TRAFFIC DISTRIBUTION – Tráfego UDP vs. TCP, distribuição relativa dos protocolos IP de acordo com o *hostname*

Estatísticas Globais de tráfego reportadas pelo NTOP:

- TRAFFIC DISTRIBUTION – Tráfego local (*subnet*) , local vs. remoto, remoto vs. local;
- PACKETS DISTRIBUTION – Número total de pacotes ordenado por tamanho dos pacotes, *unicast* vs.*broadcast* vs. *multicast* e tráfego IP vs. "*non"*-IP;
- USED BANDWIDTH – Utilização actual, média e de pico da largura de banda.
- PROTOCOL UTILIZATION AND DISTRIBUTION – Distribuição do tráfego observado de acordo com o protocolo e fonte/destino (local vs. remoto);
- NETWORK FLOWS **-** Estatísticas de tráfego para fluxos definidos pelo utilizador (tráfego de interesse particular do utilizador);
- LOCAL SUBNET TRAFFIC MATRIX – Tráfego monitorizado entre cada par de *hosts* na *subnet (*Figura 55*)*.

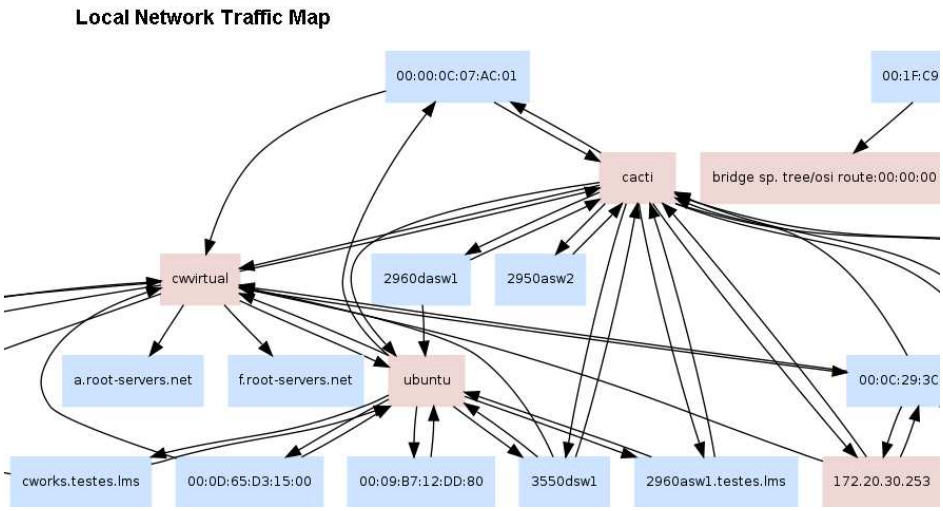


Figura 55 – NTOP, Network Traffic map

4.3 Conclusões

A implementação das ferramentas estudadas e a análise prática das potencialidades apresentadas, permitiram uma familiarização directa com as tecnologias em foco, e forneceram uma mais-valia ao nível do conhecimento que foi necessário adquirir, para resolver problemas relacionados com a execução global da instalação e configuração de todos os elementos envolvidos.

O desempenho das ferramentas no cenário montado, tendo em conta os recursos de hardware disponíveis, pode ser considerado óptimo. É pertinente referir que as condições para a implementação, foram baseadas em requisitos mínimos de operação, pelo que a transferência dos sistemas, da forma que foram implementados em laboratório, para ambientes reais, requererá recursos de hardware mais avançados, para manter o nível de desempenho observado.

A apreciação prática das ferramentas, sugeriram algumas conclusões relativas a uma futura implementação na rede informática da Universidade de Aveiro. As aplicações Cacti e Nagios, embora já se encontrem em produção, poderão apresentar melhorias na Gestão de Falhas e Desempenho, pela implementação de alguns plugins que complementam as funcionalidades básicas exploradas actualmente.

O Ntop é uma ferramenta de monitorização essencialmente passiva que actua como um sniffer, e apresenta inúmeras vantagens na Gestão de Desempenho e Segurança, mas, dada a dimensão da rede Informática da Universidade de Aveiro, uma possível implementação requererá recursos de hardware avançados para a captura de tráfego.

O CiscoWorks LMS, é uma solução completa para a gestão dos equipamentos Cisco existentes na UA, tendo como único senão, o valor comercial, pelo que uma futura aquisição, deverá ser fortemente ponderada.

5 Caso de Estudo: Operação Pega-Monstro

5.1 Introdução

O PmatE (Projecto matemática Ensino da Universidade de Aveiro), realizou no âmbito das comemorações dos seus 20 anos, o evento “Operação Pega-Monstro”, que decorreu nos dias 28,29 e 30 de Abril de 2009. Este evento englobou nove competições nacionais que congregam quatro áreas de saber – Matemática, Biologia, Física e Português (EQUAmat, DAR@língua, MINImat, MINIbio, MAISmat, mat12, bio10, bio11, bio12), e em que participaram aproximadamente 20 mil alunos do 1º, 2º e 3º ciclo do ensino básico e ensino secundário, oriundos de Portugal e Moçambique. As competições têm por base um software educativo desenvolvido pelo PmatE, e são efectuadas online através de uma aplicação Web.

Para a realização das provas, foram preparados 180 computadores portáteis (Magalhães) que durante 3 dias suportaram a interface utilizada pelos participantes.

O suporte de comunicações, serviços de rede e desktop é fornecido pelo CICUA em praticamente todos os eventos realizados na Universidade de Aveiro. Neste em particular foram empregados esforços no sentido de garantir eficácia na comunicação de dados, disponibilizando os equipamentos de switching de distribuição e acesso; a Instalação e configuração das máquinas clientes; a Instalação e configuração dos servidores que alojam serviços de rede, nomeadamente DNS e DHCP.

Em adição aos serviços prestados, foi lançado um desafio para a implementação de sistemas de monitorização com os objectivos de garantir a gestão de disponibilidade das máquinas cliente e equipamento activo, e a gestão do desempenho da rede.

5.2 Cenário

A experiencia adquirida pelo PmatE na organização das competições, fomentou a necessidade de um controlo automatizado da disponibilidade das máquinas clientes, para possibilitar aos elementos da equipa responsável pela dinamização da realização das provas, eficácia na detecção de falhas de conectividade nos computadores que suportam a interface de competição, assim como a localização espacial dos mesmos. Desta forma pretende-se que o tempo de correcção de falhas diminui-a, optimizando o decurso planeado da duração do evento.

Num cenário com milhares de participantes por dia, torna-se complicado gerir a entrada e saída das provas, dos grupos de participantes que em simultâneo as realizam. A duração das provas pode ir até aos 20, 25, 30 ou 45 minutos, e na existência de falhas nas estações de competição, 180 máquinas neste caso, o tempo para resolução de problemas deverá ser diminuto, para evitar consequências graves relacionadas com atrasos na programação do evento pondo em causa o *timing* planeado.

Do ponto de vista do equipamento activo, a importância da implementação das tecnologias de monitorização referidas é acrescida, devido ao facto de, a ocorrência de falhas nesta área poder causar o colapso da rede, indisponibilizando a conectividade de uma parte considerável, ou mesmo da totalidade, das estações de competição.

Face ao proposto, o cenário real apresentado foi constituído por:

- 180 máquinas clientes: computadores portáteis apresentados pela Iniciativa Magalhães inserida no Plano Tecnológico, baseados nos *Classmate PC,* com tecnologia Intel desenvolvida para fins educativos.
- 9 equipamentos de switching Cisco:
    - 1 Cisco Catalyst 2960G-24TC-L
    - 1 Cisco Catalyst 3550-24-EMI
    - 2 Cisco Catalyst 2950G-24-EI
    - 1 Cisco Catalyst C2960-24TT-L

  - 1 Cisco Catalyst 4000
  - 3 Cisco Catalyst 2900-24
- 20000 participantes divididos em 3 dias de competições.
- Local: tenda montada para o efeito, no Campus Universitário (Figura 56).

Figura 56 – "Operação Pega-Monstro"

5.3 Solução aplicacional

A vasta oferta existente no mercado de ferramentas de monitorização de redes, dificulta o processo de escolha das aplicações apropriadas para cenários específicos, como o exposto anteriormente. Os critérios de avaliação tidos em conta para a decisão, foram baseados na gestão de disponibilidade e desempenho pretendida para dispositivos envolvidos, nos meios disponíveis para a implementação dos sistemas, e em factores de usabilidade dos interfaces de gestão.

Os critérios designados para a escolha dos sistemas, seguiram uma estratégia baseada em níveis de abstracção:

Nível de Instrumentação:

- Gestão de informação
    - Capacidade para monitorizar todos os dispositivos e serviços envolvidos.
    - Conformidade com SNMPv2.
- Protocolos de comunicação
    - A estratégia para a recolha de informação deverá ser orientada à monitorização de conectividade de todos os dispositivos, e polling do equipamento activo para a recolha de dados referentes a tráfego.
    - Flexibilidade de acesso (suporte para gestão remota).

Nível Aplicacional:

- Sistemas operativos base
    - Suporte para Linux ou MS Windows.
- Funcionalidades das aplicações
    - FCAPS: Incidência sob as áreas funcionais Gestão de Falhas e Gestão de desempenho.
    - Suporte para personalização
    - Funcionalidades de segurança (controlo de acessos)
    - Funcionalidades para gestão de objectos (API)
- Desempenho
    - Tempo de resposta
    - Requisitos de memória
    - Eficiência: Frequência de polling

Nível do Utilizador:

- Usabilidade
    - Facilidade de aprendizagem
    - Facilidade de utilização e flexibilidade
- Visualização
    - Gestão através de interface Web

Para além dos critérios operacionais indicados, foi imposta a preferência incondicional por sistemas de licenciamento livre, possíveis de implementar com recursos de hardware modestos.

Na perspectiva apresentada, a decisão foi condicionada pela experiência profissional adquirida na área. Os sistemas escolhidos foram o Nagios e o Cacti, que de um modo geral cumprem os requisitos para a implementação no cenário referido, e oferecem vantagens a nível da existência de conhecimentos técnicos para uma implementação rápida e eficaz, e não envolverem gastos adicionais para aquisição de licenças, pois são software livre.

Nagios

Do ponto de vista dos elementos da equipa de apoio às provas, interessava a existência de um painel de monitorização que permitisse a visualização em tempo real, do estado de conectividade das máquinas cliente.

O Nagios oferece uma solução para esta necessidade, tirando proveito da flexibilidade de personalização da interface Web que disponibiliza, e pela possibilidade de configuração de alertas visuais. A estratégia de monitorização baseada no plugin "*check_ping*" possibilita independência da estação gestora em relação ao sistema cliente, devido a não ser necessária a instalação de aplicações cliente que permitissem o envio da informação pretendida. Este plugin faculta, através de suporte ICMP, a verificação disponibilidade dos dispositivos em intervalos de 1 minuto. Esta taxa de verificação de conectividade em conjunção com a capacidade de actualização da informação disponibilizada através do interface Web em intervalos de 30 segundos, oferecem uma percepção em tempo real do estado actual dos dispositivos.

Cacti

O Cacti é uma solução para monitorização de desempenho aplicável para o caso, pela capacidade que apresenta para medição de tráfego e monitorização de elementos (disco, memória, temperatura, …), a disponibilização da informação através de gráficos, e a possibilidade de configuração de notificações na ocorrência de problemas.

Para este tipo de acontecimentos, o CICUA disponibiliza uma rede dedicada, a rede de eventos, na qual a atribuição de configuração de rede pelos por parte do serviço DHCP é normalmente efectuada de forma dinâmica. A configuração do Nagios relativamente à definição de objectos correspondentes a dispositivos, requer o endereço IP ou o FQDN. Como o objectivo principal para a implementação do Nagios foi a capacidade para localizar espacialmente máquinas em que se detectam falhas de conectividade, foi necessário encontrar uma solução para a questão que surgiu no planeamento: não sendo comportável efectuar um registo estático das 240 máquinas no DHCP, assim como a configuração TCP/IP manual das mesmas, a atribuição de ip será efectuada dinamicamente, posto isto, de que forma é possível identificá-las espacialmente pelo nome FQDN? A solução encontrada foi a configuração de um DNS dinâmico que permitisse o registo das máquinas através da actualização do ficheiro de zona, efectuado pelo DHCP cada vez que este atribui um ip.

O esquema da Figura 57 solução apresenta a solução global para a implementação dos sistemas de monitorização.

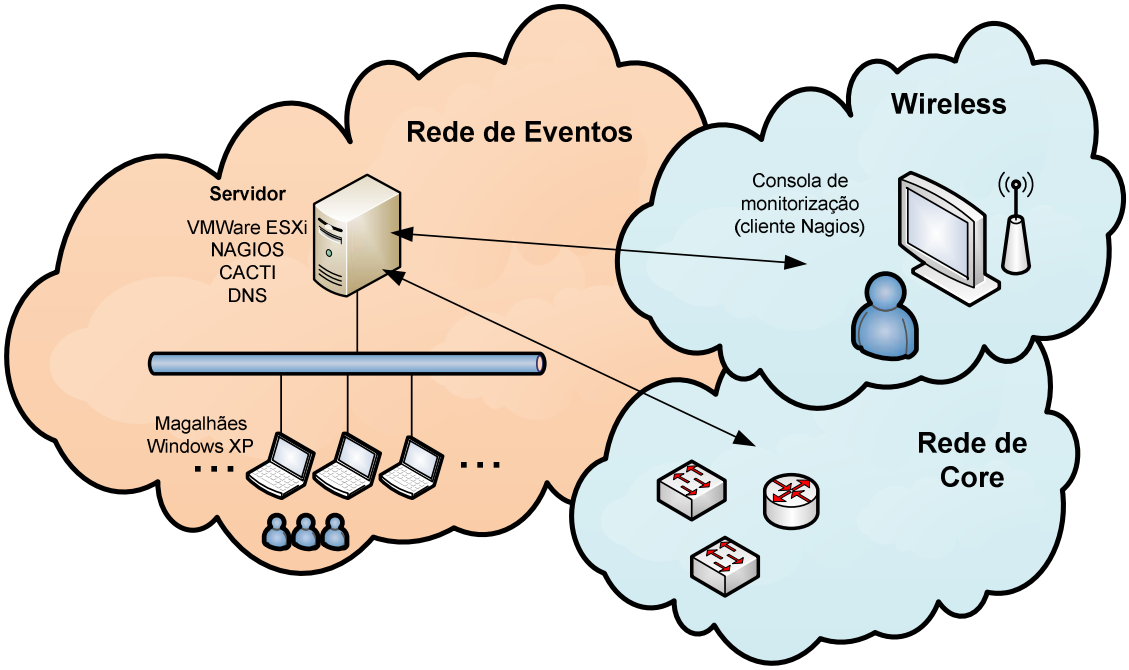


Figura 57 – Esquema do cenário "Operação pega Monstro"

Para minimizar aos recursos de hardware, pretendeu-se a utilização de apenas uma máquina para a implementação da plataforma de monitorização. Desta forma, a decisão para a escolha do sistema operativa base caiu sobre a implementação de um sistema de virtualização disponibilizado gratuitamente pela VMware, o VMware EXSi. Este sistema de virtualização corre directamente no hardware e dispensa a utilização de um sistema operativo hospedeiro, o que é vantajoso a nível de desempenho de E/S, CPU e memoria das máquinas virtuais. Outra vantagem da recorrência a uma plataforma de virtualização é a capacidade para guardar de uma forma simples cópias de segurança das máquinas “guest”, possibilitando uma reposição rápida dos sistemas no caso de inoperância de algum.

Os sistemas operativos (a implementar em máquinas virtuais) escolhidos para a instalação do Nagios e Cacti, foram distribuições Linux pela natividade agregada ao desenvolvimento destas aplicações, Ubunto Server 8.10 para o primeiro e CentOS Server 4.7 para o segundo. Desta forma optou-se também pela implementação da aplicação Bind 9 para a configuração do DDNS, em conjunto com o Nagios

5.4 Implementação

A implementação dos sistemas de monitorização foi faseada, a par com os restantes trabalhos executar, e dependente da calendarização programada para o evento, pois os 240 portáteis apenas estariam disponíveis 2 dias úteis antes da realização das provas.

Numa primeira fase foi efectuada a configuração do equipamento activo, e a preparação da plataforma de monitorização, envolvendo esta a instalação dos sistemas operativos e aplicações, assim como configurações iniciais dos serviços. Na segunda fase, coincidindo com a chegada dos portáteis, procedeu-se à montagem do equipamento activo no local, instalação do

sistema nas máquinas clientes, configurações finais do Nagios, e à realização de testes.

A ordem de trabalhos foi a seguinte:

1º fase :

- Configuração do equipamento activo:
- Instalação do servidor – sistemas operativos e aplicações
- Configuração de serviços – DHCP, DDNS, Cacti , Nagios

2ª fase

- Montagem do equipamento activo
- Instalação e configuração das máquinas
- Configuração final do Nagios

Nagios

A configuração do Nagios pode ser efectuada manualmente, através da edição de scripts de configuração ou através de diversas ferramentas gráficas disponíveis no mercado para o efeito. No sentido de compreender a estrutura orgânica do Nagios, optou-se pela configuração manual.

As primeiras tarefas de configuração dos dispositivos no Nagios foram referentes ao equipamento activo. Para isto foram criados os ficheiros que definem os dispositivos, grupos de dispositivos e dependências. O resultado destas primeiras configurações pode ser observado na Figura 58

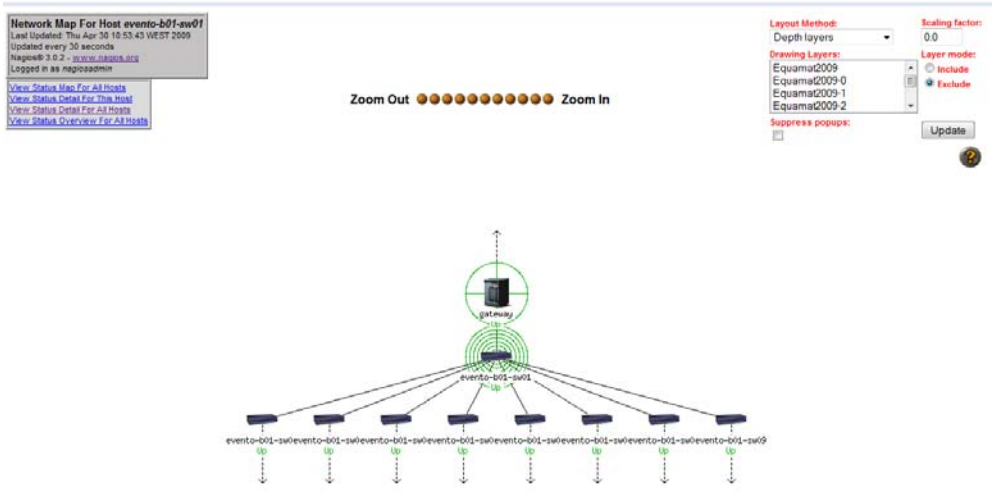


Figura 58 – Nagios, equipamento activo "Operação pega Monstro"

O passo seguinte, decorreu na altura da instalação das máquinas clientes, devido a estas já se encontrarem no local, condição necessária para a definição de coordenadas no painel personalizado.

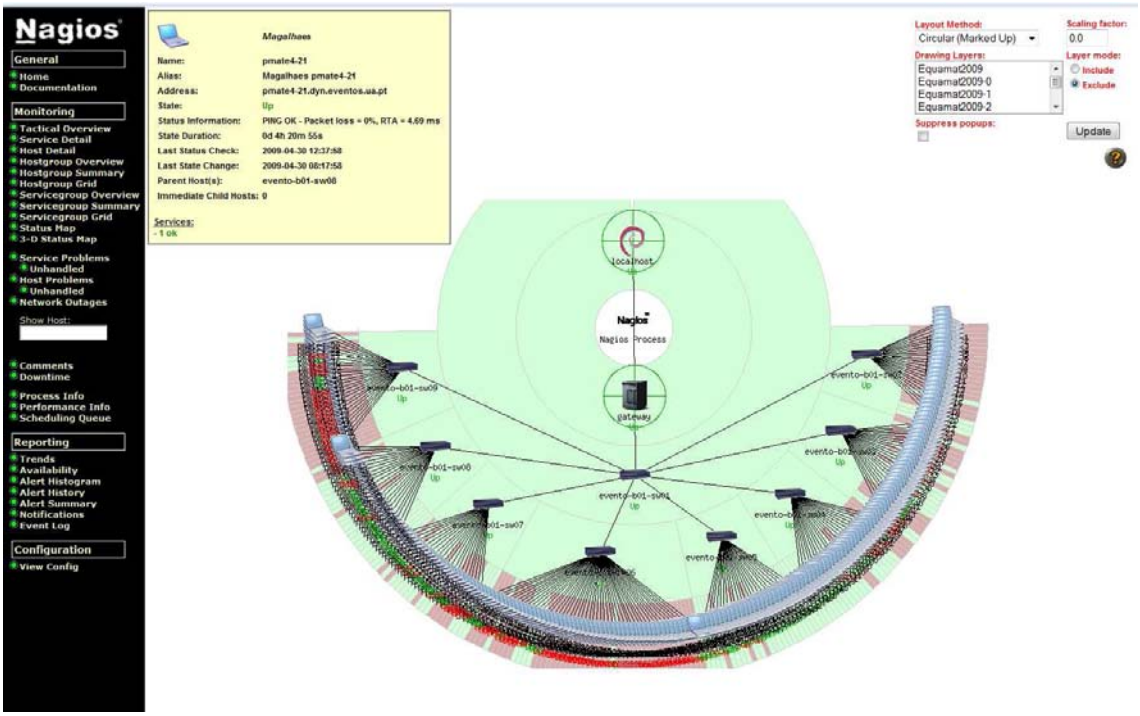


Figura 59 – Nagios, diagrama de rede "Operação pega Monstro"

~

A Figura 60 apresenta outro tipo de visualização de serviços monitorizados, por grupos de máquinas. Estes grupos correspondem aos agrupamentos de máquinas efectuados no local do evento.

Figura 60 – Nagios, Monitorização de serviços

O Objectivo principal desta implementação foi concretizado através da personalização do interface Web do Nagios pela definição de coordenadas para a localização dos objectos no painel pretendido. A Figura 61 mostra o painel de monitorização utilizado durante o evento pelos intervenientes de apoio às provas.

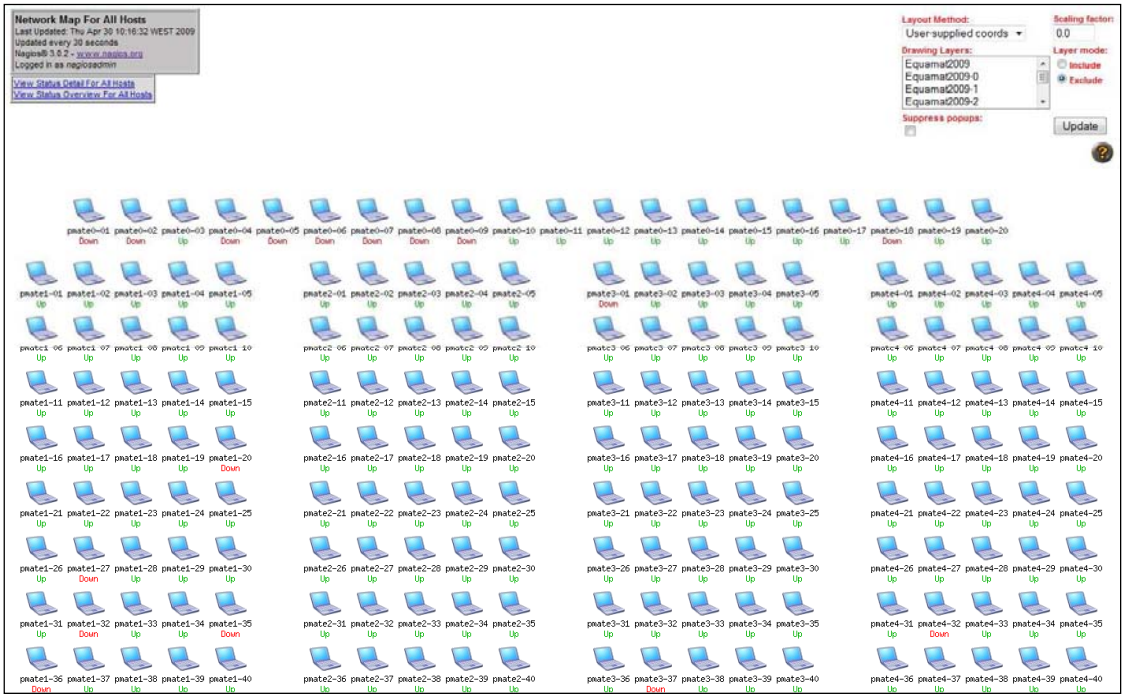


Figura 61 – Nagios, "Operação pega Monstro"

5.5 Conclusões

Toda a implementação dos sistemas de monitorização teve resultados de sucesso, não tendo sido registadas quaisquer tipos de anomalias na operação dos mesmos.

Algumas conclusões são claras pelo bom desempenho apresentado, nomeadamente a validação deste tipo de solução para cenários idênticos em eventos futuros.

Uma melhoria a propor, para aumentar usabilidade do interface gráfico que proporcionou a monitorização visual das máquinas cliente, é a programação do interface Web personalizável que contém os objectos correspondentes aos portáteis, no sentido de tornar mais notória a diferença de estados.

6 Conclusões gerais

Como já foi referido anteriormente, o emergente crescimento das TI, implica a necessidade de encontrar soluções para a gestão e monitorização das complexas infra-estruturas de rede actuais. As organizações modernas dependem das tecnologias e mecanismos de gestão disponíveis no mercado para assegurarem o bom desempenho e actividade contínua continua dos serviços que disponibilizam.

A vasta abrangência desta área dificulta a escolha das aplicações apropriadas a cada caso, tendo em conta a diversidade de tecnologias que respondem aos mesmos requisitos. A análise rápida da informação fornecida pelo competitivo e confuso mercado da gestão de redes da actualidade, relativa a produtos existentes e novas entradas, pode dar a percepção que todos estes produtos disponibilizam as mesmas funcionalidades. Torna-se essencial a compreensão das diferenças chave, competências e arquitecturas fundamentais, através uma avaliação eficaz das ferramentas de gestão de redes, na medida que os mercados de gestão de falhas e desempenho colidem na direcção da gestão ao nível de serviço. A selecção de produtos de gestão deverá ter em conta as necessidades de uma organização e requisitos necessários para a implementação, a par da estratégia fornecida pelos fabricantes a nível de escalabilidade.

As aplicações abordadas nesta dissertação cobrem apenas algumas áreas fundamentais da gestão global de uma infra-estrutura de rede, são elas a monitorização de tráfego, elementos e serviços de rede, e a gestão de equipamento activo específico (Cisco). Ficaram de fora a análise de ferramentas que suportam a gestão de sistemas, e a gestão de elementos aplicacionais. A solução completa para uma eficiente gestão de rede seria implementação de um NMS apoiado por ferramentas como as que foram aqui descritas.

Neste trabalho foi possível efectuar a avaliação de ferramentas de monitorização e gestão de redes, através uma análise e caracterização das mesmas complementadas por uma experimentação prática. Os objectivos propostos para o desenvolvimento desta dissertação foram atingidos de uma forma geral, tendo os resultados coincidido com as expectativas.

Referências

[1] Modelo OSI, Hubert Zimmermann, IEEE Transactions on Communications, vol. 28, no. 4, April 1980, pp. 425 – 432

[2] ITU-T Recommendation M.3400 , 2/2000

[3] Stallings, W., SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, Addison-Wesley 1999

[4] SNMP Research International, http://www.snmp.org/

[5] SNMP Link, http://www.snmplink.org/

[6] Ray P., Evaluation methodology for network management systems, IEEE 1998

[7] Aiko Pras, Bert-Jan van Beijnum, Ron Sprenkels, Introduction to TMN, 1999, http://wwwsnmp.cs.utwente.nl/tutorials/tmn/tmn.pdf

[8] Hegering H., Abeck S., Neumair B., Integrated Management of Network System Morgan Kaufmann Publishers, Inc. 1999.

[9] An Introductory Overview of ITIL V3, The UK Chapter of the itSMF, 2007

[10] Cacti - http://www.cacti.net/

[11] Cacti - Cacti Manual 0.8.7, http://docs.cacti.net/manual:087

[12] Cacti - http://forums.cacti.net/

[13] RRD Tool, http://oss.oetiker.ch/rrdtool/

[14] Cacti - http://cactiusers.org/index.php

[15] Nagios - Nagios Core Version 3.x Documentation, 2009, http://nagios.sourceforge.net/docs/nagios-3.pdf

[16] Chris Burgess - The Nagios Book , Chris Burgess 2005

[17] Nagios 3 Enterprise Network Monitoring Including Plug-Ins and Hardware Devices, 2008 Syngress Publishing, Inc.,

[18] Ntop: http://www.ntop.org

[19] Nagios, http:www.nagios.org

[20] CiscoWorks LMS, http://www.cisco.com/en/US/products/sw/cscowork/ps2425/index.html

[21] CiscoWorks LMS 3.2, Cisco Systems Inc, C78-534877-01, 12/2009 http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps2425/data_sheet_c78-534877.pdf

[22] User Guide for CiscoWorks LMS Portal 1.2, Cisco Systems Inc, OL-17954-01, 2009
http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lms_portal/1.2/user/guide/UserGuideforPortal.pdf

[23] CiscoWorks LAN Management Solution 3.2 Deployment Guide, Cisco Systems 2009,
http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps2425/white_paper_c07-552114.pdf

[24] User Guide for CiscoWorks Assistant 1.2, Cisco Systems Inc , OL-17904-01, 2009
http://www.ciscosystems.com/en/US/docs/net_mgmt/ciscoworks_assistant/1.2/user/guide/UserGuideforCiscoWorksAssistant12.pdf

[25] User Guide for Campus Manager 5.2, Cisco Systems Inc, OL-18011-01, 2009
http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_campus_manager/5.2/user/guide_pb/UserGuideforCM.pdf

[26] User Guide for Resource Manager Essentials 4.3, Cisco Systems Inc, OL-18664-01, 2009
https://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_resource_manager_essentials/4.3/user/guide/UserGuideforRME.pdf

[27] User Guide for Internetwork Performance Monitor 4.2, Cisco Systems Inc, OL-17965-01, 2009
http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_internetwork_performance_monitor/4.2/user/guide/UserGuideforIPM.pdf

[28] User Guide for Device Fault Manager 3.2, Cisco Systems Inc, OL-18968-01 ,2009
http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_device_fault_manager/3.2/user/guide/UserGuideforDFM.pdf

[29] User Guide for CiscoView 6.1.9, Cisco Systems Inc, OL-18716-01 ,2009
http://www.ciscosystems.to/en/US/docs/net_mgmt/ciscoworks_ciscoview/6.1.9/user/userguide/UserGuideforCV.pdf

[30] User Guide for CiscoWorks Health and Utilization Monitor 1.2, Cisco Systems Inc, OL-18094-01, 2009
http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_health_and_utilization_monitor/1.2/user/guide_12/UserGuideforHUM.pdf