Faculdade de Engenharia da Universidade do Porto

Monitorização de SLA IP

Paulo Jorge Lopes Soares Vaz

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

Orientador: Prof. João Neves

Junho de 2011

U.PORTO

FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

MIEEC - MESTRADO INTEGRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES 2010/2011

A Dissertação intitulada

"Monitorização de SLA IP"

foi aprovada em provas realizadas em 19-07-2011

o júri

Presidente Professor Doutor Manuel Alberto Pereira Ricardo
Professor Associado do Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

Professor Doutor Rui Silva Moreira
Professor Associado Faculdade de Ciências e Tecnologia da Universidade Fernando Pessoa

Professor Doutor João Manuel Couto das Neves
Professor Auxiliar Convidado do Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

O autor declara que a presente dissertação (ou relatório de projeto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extractos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são corretamente citados.

Autor - Paulo Jorge Lopes Soares Vaz

Faculdade de Engenharia da Universidade do Porto

Resumo

Com o crescimento exponencial da Internet e a sua contínua evolução, assiste-se a um aumento da importância e dependência nos serviços de rede por parte das empresas, o que as leva a procurar junto das operadoras e fornecedoras de serviços maiores garantias de desempenho e qualidade de serviço, uma vez que uma eventual falha pode ser muito prejudicial, quer ao nível financeiro, quer ao nível da competitividade da empresa.

Para tal existe o chamado *Service Level Agreement,* um contrato entre um *Internet Service Provider* e um cliente (empresa) que define quais as expectativas que ambos devem ter em termos de definição de serviços, disponibilidade, desempenho e operacionalidade do sistema.

Para essa contratualização quer o administrador da rede quer os ISP têm de saber quais as métricas a monitorizar, quem as vai monitorizar e como elas irão ser monitorizadas. Se isto não estiver bem definido pode levar a confusões sobre as responsabilidades atribuídas a cada entidade e à insatisfação com o SLA acordado.

Este projecto procura desenvolver uma ferramenta que utilizando um interface Web permita a monitorização, geração de alertas e gestão dos vários SLA contratados para circuitos ou serviços e sistemas de uma rede empresarial.

Abstract

With the exponential growth of Internet and its continuing evolution, we are witnessing an increasing importance and reliance on network services for businesses, which leads them to look at operators and service providers for greater assurance in terms of quality and performance service, since a failure can be very damaging, both financial and in terms of competitiveness.

To this end, there is the Service Level Agreement, a contract between a Internet Service Provider and a client that defines the expectations that both should have in terms of services, availability, performance and operability of the system. For such contracts, either the network administrator or the ISP has to know what metrics to monitor, how they will be monitored and those who will monitor. If this is not well defined, it can lead to confusion about the responsibilities assigned to each entity and to dissatisfaction with the agreed SLA.

This project seeks to develop a tool using a web interface that allows monitoring, alarm generation and management of various SLA contracted for circuits or services and systems in a corporate network.

Agradecimentos

Em primeiro lugar gostaria de agradecer ao meu orientador, Professor João Neves, pela forma como orientou o meu trabalho e pelas críticas e sugestões realizadas no sentido de o melhorar.

Quero também agradecer aos meus pais pelo apoio que me deram e pelo esforço que realizaram para eu poder chegar até aqui.

Agradeço aos meus colegas de curso, Victor Silva, Francisco Barbosa, Jorge Carvalho e Ricardo Faria pela ajuda que deram ao longo deste trajecto.

Por último, agradeço a todos aqueles que não foram mencionados, que sempre me apoiaram e contribuíram para o êxito deste trabalho.

Paulo Vaz

Índice

Lista de figuras

Lista de tabelas

Lista de acrónimos e abreviaturas

CLI	*Command Line Interface*
DHCP	*Dynamic Host Configuration Protocol*
DEEC	Departamento de Engenharia Electrotécnica e de Computadores
DNS	*Domain Name System*
FCAPS	*Fault, Configuration, Accounting, Performance, Security*
FEUP	Faculdade Engenharia Universidade do Porto
FTP	*File Transfer Protocol*
GPL	*General Public License*
HTML	*HyperText Markup Language*
HTTP	*Hypertext Transfer Protocol*
ICMP	*Internet Control Message Protocol*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IOS	*Internetwork Operating System*
ISP	*Internet Service Provider*
MIB	*Management Information Base*
MOS	*Mean Opinion Score*
MPLS	*Multiprotocol Label Switching*
NMS	*Network Management System*
NPM	*Network Performance Monitor*
OID	*Object Identifier*
PDF	*Portable Document Format*
PHP	*HyperText Preprocessor*
PIX	*Portuguese Internet Exchange*
QoS	*Quality of Service*
RRD	*Round Robin Database*
RTT	*Round-Trip Delay Time*
RTTMON	*Cisco Round-Trip Time Monitor*
SLA	*Service Level Agreement*
SMS	*Short Message Service*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*

SQL	*Structured Query Language*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
VoIP	*Voice over IP*
XLS	*MS Excel file extension*

Capítulo 1

Introdução

Este capítulo pretende apresentar uma visão geral do trabalho desenvolvido para a presente dissertação, através da exposição do tema abordado, descrição dos seus objectivos e finalmente a apresentação da estrutura do relatório.

1.1 Tema e Contexto

O crescimento exponencial da Internet e a sua contínua evolução, que permitiu o acesso a um novo conjunto de serviços, provocou um aumento da importância e da dependência das empresas em relação aos serviços de rede. Procuram por isso assegurar junto das operadoras e/ou fornecedoras de serviços maiores garantias de desempenho e qualidade de serviços uma vez que uma eventual falha, por mais pequena que seja, pode ser desastrosa quer ao nível financeiro quer ao nível da competitividade da empresa.

Um administrador de redes tem de controlar um sistema complexo com um número cada vez maior de equipamentos, sejam eles *routers*, *switchs* ou servidores, o que faz com que seja necessária a obtenção de informação rápida sobre problemas que tenham ocorrido ou estejam prestes a acontecer de forma a responder eficazmente e evitar falhas na rede. Desta forma a monitorização manual do sistema torna-se ineficaz e incomportável.

Assim as empresas necessitam de ter uma forma de previsão e monitorização de serviços *Internet Protocol* (IP). Aí entra o *Service Level Agreement* (SLA), que por definição é um contrato entre um *Internet Service Provider* (ISP) e um cliente que define as expectativas que ambos devem ter em termos de definição, disponibilidade, desempenho e operacionalidade de serviços garantindo assim a gestão adequada do sistema.

Com um SLA o administrador de redes tem a capacidade de definir os níveis adequados para serviços críticos e essenciais para o normal funcionamento da empresa, tendo em atenção a eficiência da rede de acordo com o tipo de utilizadores e o tipo de utilização dos mesmos procedendo então a alterações na configuração de rede baseadas em métricas de desempenho optimizadas. Conseguem também reduzir o tempo de detecção e resolução de problemas e, idealmente, verificar se o ISP está a cumprir com os níveis de serviço acordados

e contratados e em caso de falha accionar os mecanismos legais necessários para procurar ser ressarcido de eventuais prejuízos causados por uma falha com origem no ISP. Para os ISP a definição dos SLA também tem vantagens, obtêm maiores margens de lucro, aumentam a satisfação do cliente e melhoram a posição competitiva.

As métricas mais vulgares num contrato SLA para redes IP passam pela disponibilidade, fiabilidade e latência. Uma vez que a disponibilidade de serviço é fundamental para qualquer empresa, estas procuram assegurar junto dos ISP níveis de disponibilidade de serviço altos para que os tempos de *downtime* sejam os mais reduzidos possíveis. Essa disponibilidade, tal como descrito em [1] pode ser expressa como uma percentagem de *uptime* por ano, mês, semana, dia ou hora comparada com o tempo total desse período. Empresas com uma estrutura e necessidades maiores poderão mesmo ter a necessidade de procurar garantir um nível de disponibilidade de 99,999%, os chamados "cinco noves", que tal como se encontra indicado na Tabela 1.1, indica cinco minutos de *downtime* ao ano.

Tabela 1.1 - Disponibilidade: Tempo de *downtime* em minutos

Disponibilidade	Hora	Diária	Semanal	Anual	Anual (Horas)
99,999%	0,0006	0,01	0,1	5	
99,98%	0,012	0,29	2	105	1h 45min
99,95%	0,03	0,72	5	263	4h 23min
99,90%	0,06	1,44	10	526	8h 46min
99,70%	0,18	4,32	30	1577	26h 17min
99,50%	0,3	7,2	50,4	2628	43h 48min

Algo que para se conseguir obter implica tripla redundância, isto é, ter acesso à rede a partir de três ISP diferentes, tal como apresentado na Figura 1.1, de forma a garantir que em caso de falha de uma delas as outras duas suportem o funcionamento normal da empresa.

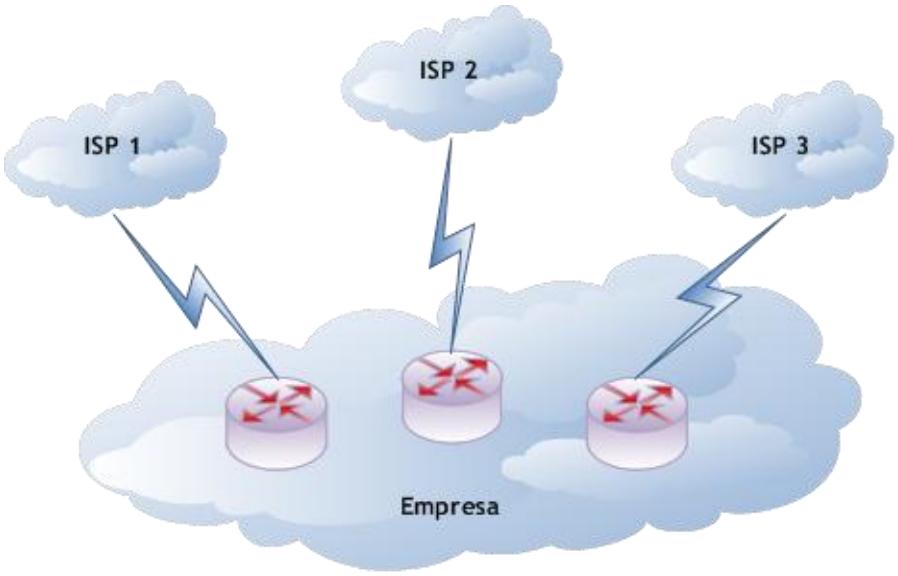


Figura 1.1 - Tripla redundância de rede, em [1]

Em termos de latência e fiabilidade, um tempo de atraso elevado ou a existência de perda de pacotes na rede pode tornar inviável a utilização de algumas aplicações sensíveis a estas métricas. Aplicações em tempo real como o *voice over IP* (VoIP) e videoconferência podem ser afectadas negativamente com a existência de perda de pacotes e/ou de um atraso elevado, pelo que as empresas procuram garantir o mínimo valor possível destas métricas num contrato de SLA.

No entanto este tipo de soluções, necessita de ser controlada quer pelo ISP, mas também e principalmente pela empresa que tem a necessidade de garantir que o acordo está a ser cumprido devido aos possíveis prejuízos que um incumprimento pode causar. Logo se juntarmos ao custo da garantia de níveis de serviço mais elevados, o custo da implementação e desenvolvimento de soluções de monitorização e gestão de serviços pode levar a que uma empresa seja incapaz de suportar os custos associados a este conjunto de soluções.

1.2 Objectivo

O objectivo desta dissertação passou por desenvolver uma ferramenta que permitisse monitorizar e gerir os SLA contratados para circuitos ou sistemas de uma rede empresarial.

Esta ferramenta resultou da integração e configuração de ferramentas o*pen source*, utilizando um interface Web que permitiu a monitorização, geração de alertas e gestão dos vários SLA definidos para serviços e sistemas na rede.

1.3 Estrutura da dissertação

Este relatório encontra-se organizado em seis capítulos.

No primeiro capítulo é descrita a motivação para o desenvolvimento desta dissertação e os objectivos da mesma.

No segundo capítulo é descrito o que são SLAs e IP SLAs fazendo referência a métricas típicas, operações suportadas e a sua evolução.

No terceiro capítulo são apresentadas soluções actuais, disponíveis no mercado, para a monitorização de SLAs IP.

No quarto capítulo é feita a caracterização e implementação da solução desenvolvida ao longo do trabalho.

No quinto capítulo são apresentados os resultados obtidos pela solução implementada.

No sexto capítulo é apresentada uma síntese do trabalho desenvolvido e as melhorias possíveis que podem ser introduzidas em desenvolvimento futuro.

No final é apresentada a lista de todas as referências utilizadas no desenvolvimento deste trabalho.

Capítulo 2

Service Level Agreements – Objectivos, descrição e problemas

Neste capítulo é descrito o que são SLAs e IP SLAs fazendo uma breve apresentação sobre os objectivos, desenvolvimento e problemas.

2.1 Objectivos e processo de desenvolvimento

Os objectivos de um SLA passam por ser um meio de prevenção e resolução de potenciais conflitos e de definição de níveis de qualidade de serviço entre um ISP e um cliente. Deve ser definido de acordo com as características dos serviços pretendidos pelo cliente e especificam as obrigações que clientes e ISP devem respeitar em termos de desempenho, disponibilidade e segurança de serviços bem como os procedimentos a realizar em caso de falha. Pode ser especificado tanto para serviços já utilizados pelo cliente, ou para sistemas que ainda nem sequer foram projectados.

O processo de desenvolvimento de um SLA passa pela identificação das necessidades do cliente, pela determinação dos níveis de serviço necessários, pelo acordo entre cliente e ISP ao nível de serviços e prevenção de conflitos, pela definição de regras de colaboração entre ambas e a especificação de regras de actuação em caso de falhas.

2.2 Descrição

Um SLA é a formalização de *Quality of Service* (QoS) num contrato entre um cliente e um ISP, tal como descrito em [1]. Geralmente um SLA, tal como é descrito em [2] é composto pela descrição do serviço a ser disponibilizado, pela descrição do nível de desempenho do serviço definindo parâmetros como fiabilidade, disponibilidade e latência, pela definição das

condições que permitem ao ISP não respeitar, num determinado momento, os níveis de serviço acordados, pela descrição de procedimentos para comunicação e aceitação de problemas, desde entidade a contactar até à forma de apresentação formal do problema, pela definição de tempo máximo de resposta (tempo desde que o problema é comunicado pelo cliente, até que alguém do ISP o comece a resolver) a um problema, pela definição de tempo máximo de resolução de um problema e pela descrição das penalizações em caso de falha no cumprimento das obrigações acordadas, desde indemnizações até condições para rescisão de contrato.

Um SLA deverá assim apresentar uma visão geral dos diferentes parâmetros que compõem os serviços contratados, as situações em que podem ocorrer falhas e como resolvê-las, procurando encontrar um equilíbrio entre as necessidades e expectativas do cliente e aquilo que o ISP pode ou quer fornecer.

Um SLA deve ser especificado em termos de eficiência e características de negócio, tendo em conta o conhecimento das necessidades do utilizador e as características do negócio de uma empresa de forma a identificar correctamente as prioridades e o peso relativo dos elementos de um SLA. Deve ser efectuado de forma organizada e estruturada de forma a evitar tomadas de decisões precipitadas que possam levar à obtenção de um SLA desfasado da realidade do cliente, ou incompleto, devendo ser baseado em elementos como disponibilidade, desempenho, apoio ao utilizador e prevenção de falhas, devendo ser usados termos que aumentem o nível de compreensão por parte do cliente e dessa forma limitar os problemas e conflitos que especificações subjectivas podem provocar e também deve ter conta que diferentes grupos de utilizadores têm diferentes necessidades, o que deve levar a uma diferenciação de serviços e a uma mais eficiente utilização destes.

2.3 Problemas

Tal como descrito em [3] os SLA apresentam alguns problemas que passam por apenas referir o esforço que um ISP tem de despender em caso da ocorrência de falhas na rede, não existindo referências para os objectivos que um dado serviço deve cumprir, a definição de problema, ou falha pelo ISP não tem como base a altura em que este ocorre, mas geralmente quando é que ele é comunicado pelo cliente e em muitos casos quando é que a ocorrência é aberta pelos serviços técnicos, alguns dos termos utilizados na especificação dos elementos de um SLA podem ser de difícil compreensão. Por exemplo, será que um cliente sabe o que quer dizer uma disponibilidade de serviço de 98%? Saberá qual a diferença entre disponibilidade de 98% ou 99%?

Outros problema passa pela relação preço/desempenho de serviços para o cliente não ser optimizada, uma vez que não vem indicado qual o custo que um determinado serviço possuí, ou como é que esse custo está relacionado com as necessidades do cliente.

Como consequência, um SLA pode torna-se um documento de difícil compreensão, restrita apenas a um pequeno conjunto de pessoas com formação técnica superior, o que pode levar a confusões sobre as responsabilidades atribuídas, à dificuldade de interpretar correctamente os parâmetros de serviços acordados e à insatisfação do cliente com o SLA acordado.

2.4 SLA em Redes IP

Tal como descrito em [2] no contexto das redes IP um SLA pode ser fornecido para três tipos de ambientes, serviços de conectividade de rede, serviços de alojamento e serviços de integração entre os serviços de conectividade e alojamento, sendo que os recursos de rede são fornecidos para cumprir os objectivos de desempenho e disponibilidade desejados, reduzindo dessa forma o custo operacional sem provocar um impacto negativo na satisfação do cliente.

Nos serviços de conectividade de rede, as redes dos clientes encontram-se ligadas directamente à rede do ISP. Para este tipo de redes os limites de disponibilidade e desempenho passam pela latência na rede do ISP para *peering* directo, para o Centro de Troca de Tráfego, para tráfego Intracontinental e para tráfego Intercontinental, pelo nível de disponibilidade de serviço e pelo nível de fiabilidade de serviço.

Serviços de alojamento são oferecidos por operadores que suportam e alojam os diferentes tipos de servidores dos seus clientes. Estes serviços vão desde alojamento de sítios Web (*Web Hosting*), locais para armazenamento e manutenção de servidores ou dos conteúdos e aplicações alojadas no sítio.

Os SLA oferecidos para este tipo de serviços passam pelos tempos de *uptime* e o nível de desempenho dos servidores que estão a ser alojados. Estes operadores controlam apenas as comunicações do lado do servidor, não têm nenhum controlo sobre as comunicações do lado do cliente, nem sobre o desempenho da rede. Pode também alojar múltiplos clientes num mesmo sítio e dessa forma é responsável por assegurar que a performance de um servidor de um cliente não é afectada pelos pedidos direccionados a outros clientes.

Elementos típicos de performance e disponibilidade são o tempo de indisponibilidade de um servidor alojado, o número de pedidos que um servidor pode suportar, o número mínimo de servidores disponíveis em todo o momento e a taxa de transferência suportada para um determinado servidor.

Um terceiro tipo de serviço fornece um serviço consolidado em que o ISP controla a rede bem como a infra-estrutura de alojamento. Alguns elementos presentes num SLA são o tempo máximo de pesquisa e o tempo de *downtime* não programado do servidor de correio electrónico.

Em todos estes ambientes operacionais, a natureza dos serviços fornecidos, os objectivos de desempenho e disponibilidade e os mecanismos usados para monitorizar o desempenho dos serviços é diferente, mas os componentes dos SLA são relativamente semelhantes.

Capítulo 3

Estado da Arte

Neste capítulo são apresentadas soluções actuais, disponíveis no mercado, para a monitorização de SLA IP.

3.1 Cisco IOS IP Service Level Agreements

Tal como indicado em [4] e [5], a Cisco também apresenta uma solução para monitorização de SLA, a Cisco *Internetwork Operating System* (IOS) IP *Service Level Agreement*, uma funcionalidade para monitorização de desempenho de rede em equipamentos Cisco. Com esta solução a Cisco permite verificar os níveis de serviço contratados, o nível de desempenho da sua rede, a análise e resolução de problemas procurando dessa forma aumentar a fiabilidade da rede. Utiliza monitorização de tráfego activa, geração de tráfego de forma contínua e fiável, enviando dados pela rede para medir o desempenho entre múltiplas localizações ou por diferentes caminhos na rede, simulando serviços IP e recolhendo informação em tempo real. Essa informação passa por dados estatísticos sobre tempos de resposta de rede, latência, *jitter*, perda de pacotes e tempo de resposta de servidores.

Apesar de muitos dos protocolos utilizados pela Cisco serem standards *Internet Engineering Task Force* (IETF), esta a solução não é um standard IETF, mas que tem a característica de poder ser usada não só entre equipamentos Cisco, mas também tendo um equipamento Cisco na origem e como destino um equipamento IP remoto, podendo monitorizar o desempenho em qualquer ponto da rede sem necessidade de utilização de equipamentos ou software adicional. Pode-se recolher ou analisar os valores através dos comandos da Cisco, por consola ou *Command Line Interface* (CLI), por *Simple Network Management Protocol* (SNMP), *Cisco Round-Trip Time Monitor* (RTTMON) ou através da análise do *syslog* de *Management Information Bases* (MIBs).

Como os dados são acedidos por SNMP, também podem ser usadas ferramentas de monitorização de rede, com o uso das Cisco RTTMON MIBs para interacção com essas ferramentas.

A Figura 3.1 ilustra o seu funcionamento, onde a partir da origem é enviado um pacote para o equipamento de destino, que após o receber e tendo em conta o tipo de operação a que está associado responde com a informação necessário para na origem ser calculada o valor da métrica

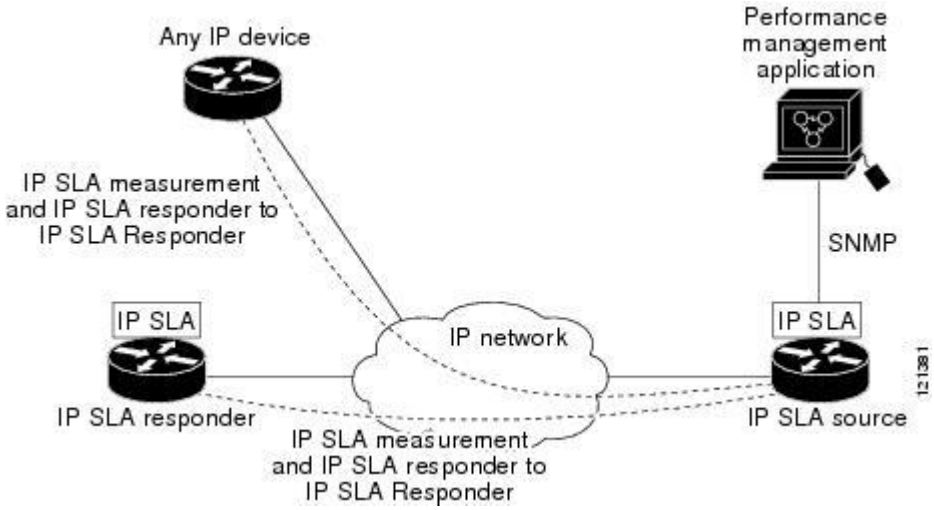


Figura 3.1 – Funcionamento Cisco IP SLA, em [6]

Esta solução, tal como indicado em [7] procura assegurar aos seus utilizadores a monitorização e verificação de SLAs, a monitorização de desempenho e disponibilidade da rede, a medição de parâmetros como *jitter*, latência e perda de pacotes na rede, a monitorização de nível de desempenho do serviço VoIP e a monitorização de nível de desempenho de *Multiprotocol Label Switching* (MPLS) e *Virtual Private Network* (VPN).

Sendo que para a sua implementação é necessário realizar um conjunto de tarefas que passam pela activação, nas operações exigidas do IP SLA Responder, pela configuração das operações, pela configuração das opções disponíveis para a operação IP SLA especificada, pela calendarização da execução da operação e o período de tempo em que recolhe estatísticas e pela apresentação dos resultados da operação através dos comandos Cisco ou num sistema de *Network Management System* (NMS) com SNMP.

O IP SLA Responder é um componente presente apenas nos equipamentos Cisco que permite ao sistema antecipar e responder aos pedidos. Deve ser configurado nos equipamentos de destino de uma operação IP SLA, mas não é obrigatório para todos os tipos de operações. O protocolo de controlo de IP SLAs é usado para que o responder seja notificado de que porta deverá escutar e responder. Ele numa porta específica escuta as mensagens de controlo enviadas por uma operação e quando as recebe irá activar a porta especificada (seja *Transmission Control Protocol* (TCP) ou *User Datagram Protocol* (UDP)) durante um período fixo de tempo. Depois irá aceitar pedidos e responde-los, sendo que desactiva a porta quando envia a resposta ou o período de tempo especificado expira. Para equipamentos que não sejam Cisco não é possível a sua configuração pelo que o IP SLA apenas envia pacotes de serviços nativos desses aparelhos.

Resumindo, a utilização desta solução está orientada para a visualização do desempenho de serviços de VoIP, vídeo, MPLS e redes VPN, para a monitorização de SLAs, desempenho e disponibilidade da rede e do desempenho de aplicações, para a avaliação do estado dos serviços da rede e para a resolução de problemas operacionais da rede.

As principais métricas a testar passam pelo atraso, *jitter*, perda de pacotes e sequenciação de pacotes, conectividade, caminho, tempo de transferência de ficheiros de servidores ou sítio Web e qualidade de voz, de forma a garantir monitorização de desempenho VoIP, de disponibilidade e desempenho de aplicações e equipamentos, de tempo de resposta de servidores, de desempenho de servidor de DNS, DHCP, FTP e desempenho de sítios Web.

Os principais tipos de operação suportados são o *Internet Control Message Protocol* (ICMP) *Echo*, o ICMP *Jitter*, o ICMP *Path Echo*, o ICMP *Path Jitter*, o UDP *Echo*, o UDP *Jitter*, o *Domain Name System* (DNS), o *Dynamic Host Control Protocol* (DHCP), o *File Transfer Protocol* (FTP), o *Hypertext Transfer Protocol* (HTTP), e o TCP *Connect*.

Uma vez que um router pode demorar algum tempo a processar os pacotes que lhe chegam, devido a outros processos com maior prioridade, e dessa forma afectar os tempos de resposta reais das operações, esta solução utiliza *time stamping* nos seus pacotes de teste de forma a minimizar esses atrasos no processamento e garantir valores reais de *Round-Trip Time* (RTT).

Após a configuração tem-se de iniciar a operação de forma a esta começar a recolher a informação pretendida, podendo-se indicar quando deve começar, se imediatamente, ou daqui a um dia ou mês e quando é que deve parar a sua recolha permitindo assim um maior controlo na quantidade de tráfego gerado. Um exemplo do comando utilizado e apresentado de seguida:

ip sla schedule id start-time now life forever

Em que o utilizador configura a operação SLA com número de identificação 1 a começar imediatamente por tempo indeterminado.

Nos seus parâmetros de configuração pode-se indicar o tipo de estatísticas a ser apresentadas. Por defeito é apresentada a última informação disponível, mas também é possível configurar para ver um histórico agregado para um determinado período definido ou também apresentar uma distribuição de frequência a partir de intervalos configuráveis.

Todos os equipamentos Cisco que correm *Cisco IOS Software* suportam a *Cisco IOS IP SLAs* com a excepção da *Cisco Catalyst 4500 Series Switch*.

Na Figura 3.2 é ilustrado um resumo das funções, métricas e operações suportadas por esta tecnologia.

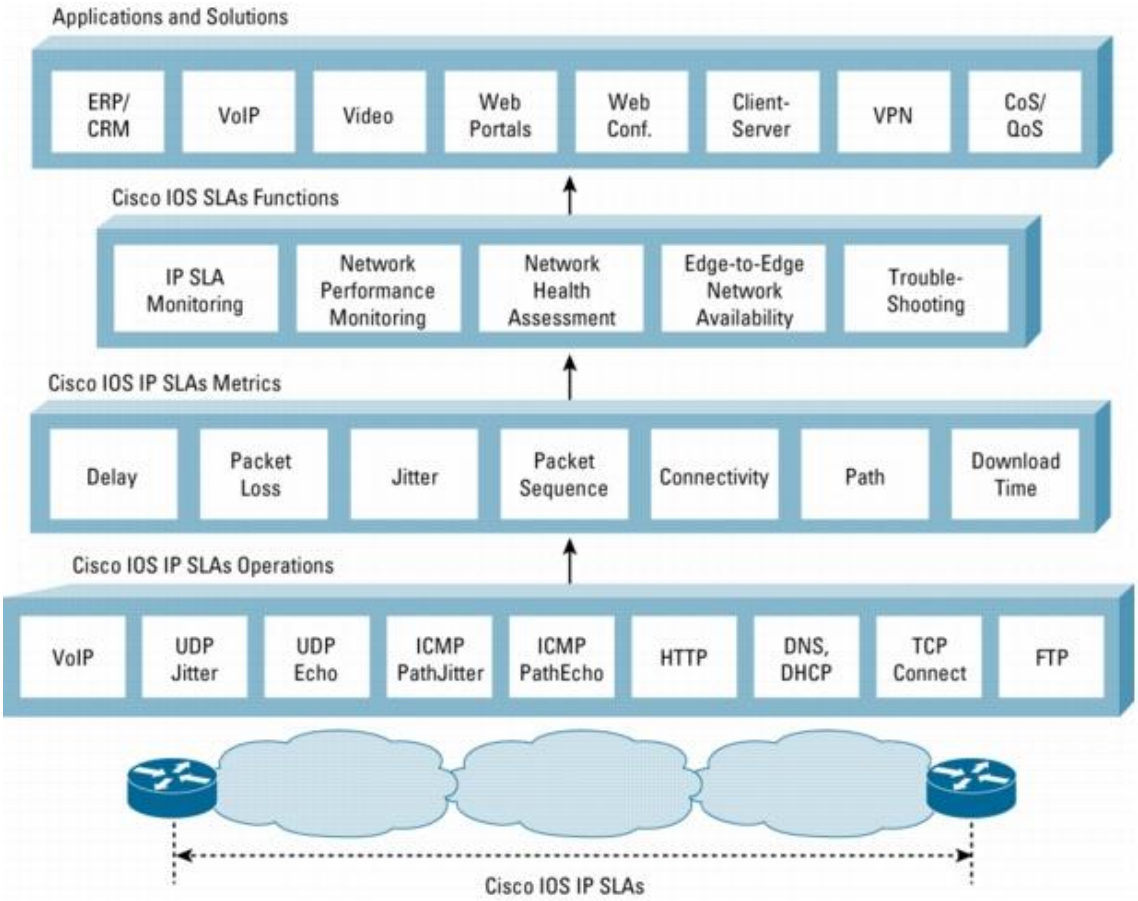


Figura 3.2 – Cisco IOS IP SLA funções, métricas e operações, em [8]

De seguida são apresentadas algumas das operações suportadas pela Cisco IOS IP SLA.

3.1.1 Operação ICMP-Echo

Esta operação, apresentada em [9] é útil para monitorizar problemas de conectividade da rede uma vez que monitoriza o RTT entre um router Cisco e um qualquer equipamento IP que use IPv4 ou IPv6. Pode ser usado como destino um qualquer equipamento de rede que suporte o protocolo RFC 862, o protocolo *Echo*.

O RTT é obtido através da medição do tempo que leva entre o envio de uma mensagem ICMP *Echo request* para o destino e a recepção da resposta, uma mensagem ICMP *Echo reply*.

Esta operação utiliza as mesmas especificações IETF que o comando ping, pelo que os dois métodos resultam nos mesmos tempos de resposta.

O comando deste tipo de operação é

icmp-echo (IP destino | hostname destino) source-ip (ip | hostname)

Na Figura 3.3 é apresentado o funcionamento desta operação.

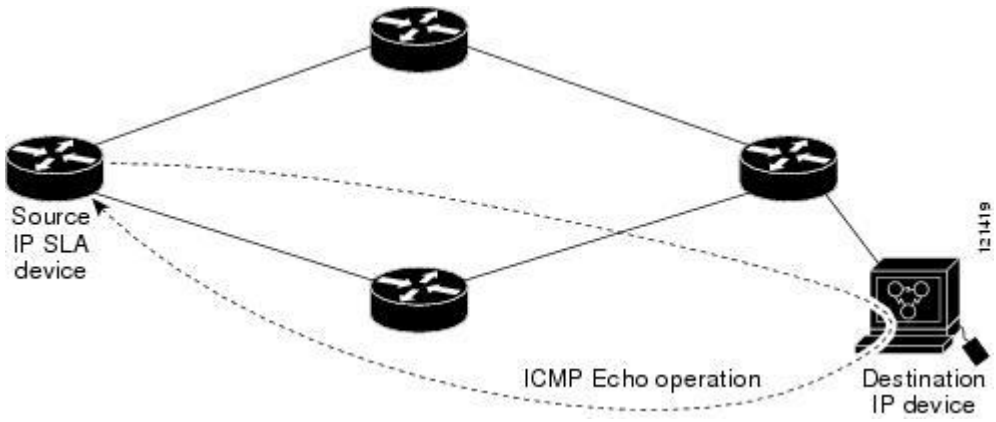


Figura 3.3 – Operação ICMP-Echo, em [10]

Obtêm-se como resultados:

IPSLA operation id: 1
Type of operation: icmp-echo
Latest RTT: 1 milliseconds
Latest operation start time: 13:01:02.082 GMT Fri Jun 10 2011
Latest operation return code: OK
Number of successes: 15
Number of failures: 0
Operation time to live: Forever

Figura 3.4 – Resultados operação ICMP-Echo

3.1.2 Operação HTTP

Esta operação, apresentada em [11] serve para determinar o desempenho de um servidor de HTTP. Para tal, monitoriza o tempo de resposta para obter uma página Web entre um equipamento Cisco e um servidor http. Tem suporte para pedidos GET ou RAW.

O tempo de resposta consiste de três tipos e é feita pela seguinte ordem:

- RTT DNS *lookup*;
- RTT TCP *Connect*: tempo que demora a efectuar uma conexão TCP com o servidor;
- RTT HTTP *transaction time*: tempo que demora o envio de um pedido e a obtenção de resposta de um servidor de http, sendo que apenas a pagina inicial *HyperText Markup Language* (HTML) é obtida.

O tempo total é a soma destes três tempos. Obtém-se como resultados:

IPSLA operation id: 2
Type of operation: http
Latest RTT: 6 milliseconds
Latest operation start time: 13:01:02.082 GMT Fri Jun 10 2011
Latest operation return code: OK
Latest DNS RTT: 0 ms
Latest TCP Connection RTT: 2 ms
Latest HTTP Transaction RTT: 4 ms
Number of successes: 14
Number of failures: 0
Operation time to live: Forever

Figura 3.5 – Resultados operação HTTP

3.1.3 Operação DNS

Esta operação, apresentada em [12] é usada para determinar o tempo de DNS *lookup*, que é determinante para verificar o nível de performance de um servidor DNS ou Web, tempos de DNS *lookup* mais rápidos traduzem-se num acesso mais rápido a um servidor Web. Ela mede a diferença de tempo entre o envio um DNS *request* e a recepção da resposta.

A operação de DNS faz uma *query* a um endereço IP se for especificado um *hostname* ou faz uma *query* ao *hostname* se for especificado um endereço IP.

O comando para realizar esta operação é:

dns (IP | hostname destino) name-server (IP) source-ip (IP | hostname)

Na Figura 3.6 é apresentado como é realizada a operação DNS IP SLA

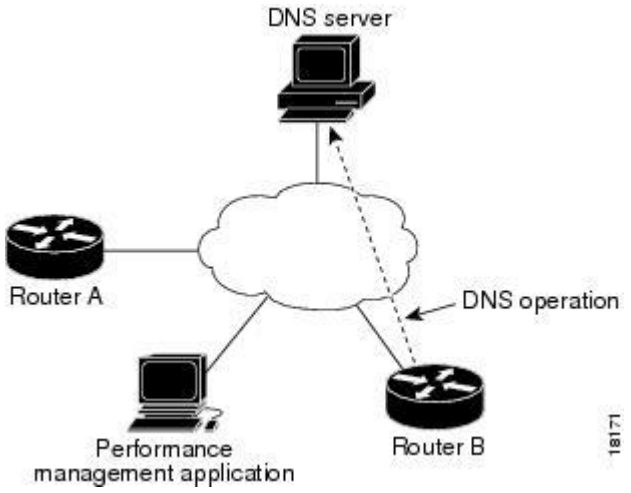


Figura 3.6 – Operação DNS, em [13]

Obtêm-se como resultados:

```
IPSLA operation id: 3
Type of operation: dns
        Latest RTT: 10 milliseconds
Latest operation start time: 13:01:02.082 GMT Fri Jun 10 2011
Latest operation return code: OK
Number of successes: 93
Number of failures: 0
Operation time to live: Forever
```

Figura 3.7 – Resultados operação DNS

3.1.4 Operação DHCP

Esta operação, tal como é apresentada em [14] é usada para determinar os níveis de desempenho do DHCP. Ela mede o RTT para descobrir um servidor DHCP e obter um endereço IP a partir dele, sendo que esta operação liberta o endereço IP depois de concluída.

Tem dois modos de operação, um que envia pacotes DHCP *Discover* em todas as interfaces IP do router, ou um segundo em que se um servidor DHCP for configurado no router todos os pacotes serão enviados apenas para servidor específico.

O comando é:

dhcp (IP | hostname destino) source-ip (IP | hostname)

Obtém-se como resultados:

```
IPSLA operation id: 4
Type of operation: dhcp
        Latest RTT:  128 milliseconds
Latest operation start time: 13:01:02.082 GMT Fri Jun 10 2011
Latest operation return code: OK
Number of successes: 83
Number of failures: 0
Operation time to live: Forever
```

Figura 3.8 – Resultados operação DHCP

3.1.5 Operação FTP

A operação FTP apresentada em [15] serve para determinar o nível de desempenho de um servidor FTP ao medir o RTT entre um equipamento Cisco e um servidor FTP para a retirada de um ficheiro podendo também ser usado para a resolução de problemas relacionados com o desempenho de um servidor FTP. Apenas suporta pedidos FTP GET, mas tem suporte para modo de transferência activo e passivo, sendo que por defeito o modo de transferência é o passivo.

O URL especificado na operação FTP GET tem de ter um dos seguintes formatos

- ftp://nome_utilizador:palavra_passe@*host*/nome_ficheiro
- ftp://*host*/nome_ficheiro

O comando para a sua configuração é:
ftp get url [source-ip {ip-address | hostname}] [mode {passive | active}

Na Figura 3.9 é ilustrado como é realizada a operação FTP IP SLA

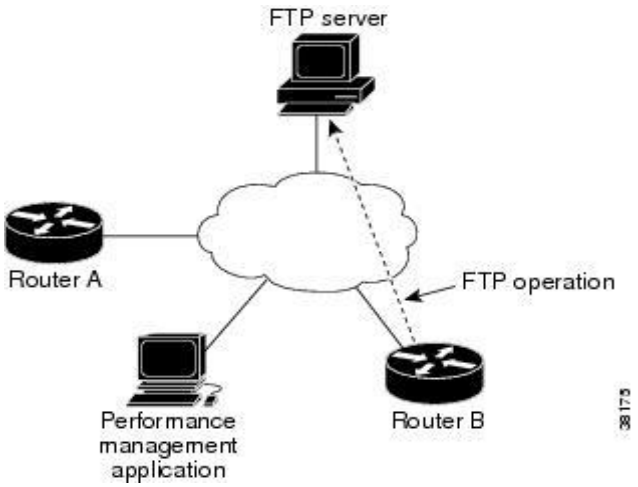


Figura 3.9 – Operação FTP, em [16]

Obtém-se como resultados:

IPSLA operation id:
Type of operation: ftp
Latest RTT: 30 milliseconds
Latest operation start time: 13:01:02.082 GMT Fri Jun 10 2011
Latest operation return code: OK
Number of successes: 100
Number of failures: 0
Operation time to live: Forever

Figura 3.10 – Resultados operação FTP

3.2 Ferramentas de monitorização comerciais

3.2.1 *Orion* IP SLA *Manager*

A *Solarwinds* [17], oferece uma solução para monitorização de redes o *Orion Network Performance Monitor* (NPM) [18], que possuí um módulo, o *Orion* IP SLA *Manager* apresentado em [19], que permite a monitorização de estatísticas de desempenho de um router utilizando para isso a tecnologia IP SLA da Cisco. Este módulo permite a identificação dos equipamentos de rede que suportam esta tecnologia, a configuração automática de operações IP SLA, e a visualização dos níveis de desempenho de várias métricas, tudo isto a partir de uma interface Web que elimina a necessidade de utilização da CLI. As operações suportadas são, HTTP, FTP, DNS, DHCP, TCP *Connect*, UDP *Jitter*, VoIP UDP *Jitter*, ICMP *Echo*; UDP *Echo*, ICMP *Path Echo*, ICMP *Path Jitter*.

As suas principais características são o aproveitamento da tecnologia já existente nos routers Cisco, pela visualização de estatísticas de desempenho da rede, pela descoberta automática de equipamentos com suporte da tecnologia Cisco IP SLA, pela configuração automática de operações IP SLA nos equipamentos, pela monitorização simultânea de múltiplas operações em múltiplos equipamentos, pela configuração de *thresholds* para cada operação e de alertas visuais em caso de incumprimento de *thresholds*, pelo envio automático de relatórios por *email* e pela monitorização de estatísticas de desempenho da Cisco VoIP, tais como *Mean Opinion Score* (MOS), VoIP *jitter*, latência e perda de pacotes.

3.2.2 *Redcell Advanced Monitor* – Cisco IP SLA

A *Dorado software*, [20], também disponibiliza uma ferramenta que aproveita a tecnologia Cisco IP SLA, o *Redcell Advanced Monitor* – Cisco IP SLA [21], integrada nas suas soluções de gestão de serviços.

Esta ferramenta permite guardar os dados obtidos pelas operações IP SLA, configurar notificações para latência elevada, baixos valores de MOS e outros valores disponíveis e alertas, quando o *threshold* indicado para uma métrica é ultrapassado. Todas as operações da Cisco IP SLA estão disponíveis para ser acedidas por esta ferramenta.

3.2.3 *Nimsoft Monitor*

Esta ferramenta disponibilizada pela *Nimsoft* em [22], permite a monitorização e configuração automática de equipamentos aproveitando a tecnologia IP SLA da Cisco. Possui uma interface centralizada que permite gerir, criar e apagar testes IP SLA e monitoriza valores de RTT, latência, *jitter* e perda de pacotes. Como aproveita uma tecnologia já

existente nos equipamentos Cisco não é necessária a inclusão de nenhum outro software nesses equipamentos.

As suas principais características são a monitorização do desempenho DHCP, DNS, FTP, FTP, HTTP, UDP e TCP, a monitorização de valores de atraso, *jitter* e perda de pacotes, a configuração centralizada, dispensando a utilização da CLI para configuração de operações IP SLA e a possibilidade de envio de notificações por *email* e por *Short Message Service* (SMS).

As operações IP SLA suportadas são DHCP, DNS, ICMP *Echo*, FTP, HTTP, UDP *Jitter*, UDP *Echo* e TCP *Connect*.

3.2.4 EYE – *Eye of the Storm Entreprise*

Esta é uma ferramenta desenvolvida pela *Entuity* [23], para gestão de redes. Possuí um módulo o EYE IP SLA Module, que tal como descrito em [24] utiliza a tecnologia Cisco IOS IP SLA para recolha e monitorização de dados de desempenho de rede como latência, *jitter* e perda de pacotes.

Permite a detecção de equipamentos com suporte a esta tecnologia e a configuração automática de operações IP SLA tornando desnecessário a utilização da CLI para este tipo de configurações, sendo necessário que no equipamento exista permissão de escrita por SNMP. As operações suportadas são DHCP, DNS, HTTP, ICMP *Echo*, ICMP *Path Echo*, TCP *Connect*, UDP *Echo* e UDP *Jitter*. Como é uma ferramenta que já utiliza os recursos presentes nos equipamentos Cisco não precisa de nenhum tipo de software adicional para realizar esta tarefa. Possui suporte VoIP através de previsão de valores de ICPIF e MOS para operações *Jitter* e emulação de *codecs* de voz.

Permite a visualização de eventos e envio de notificações a partir de outros módulos desta ferramenta, no caso o EYE *Event Viewer* e o EYE *Reports*.

3.3 Ferramentas de monitorização *open source*

3.3.1 *Nagios*

O *Nagios* [25] é uma ferramenta *open source* para monitorização de sistemas de rede, desenhada para correr em ambientes Unix e licenciada nos termos da licença GNU *General Public License* (GPL) versão 2, sendo por isso um software livre.

Faz a monitorização de serviços de rede como o *Simple Mail Transfer Protocol* (SMTP), HTTP, ICMP, SNMP FTP e DNS bem como a monitorização de recursos (como carga do processador ou utilização de disco) de diversos tipos de equipamentos como servidores (Windows ou Unix), *routers, switches* ou impressoras.

Tal como indicado em [26] e [27], apresenta informação ou através de um pagina Web, ou através de e-mail ou mesmo por SMS de acordo com os parâmetros definidos pelo administrador da rede que está a ser monitorizada.

O *Nagios* apresenta uma estrutura modular, utilizando programas externos, criados geralmente por elementos da comunidade, que adicionam novas funcionalidades de monitorização, informação e notificação, melhorando o seu desempenho e tornando-o uma ferramenta mais poderosa. Esses programas são denominados de *plugins*, e podem ser obtidos em [28] e [29]. Estes *plugins* são executados quando é necessário verificar o estado de um *host* ou serviço retornando os resultados para o *Nagios*, que por sua vez processa esses resultados e toma as medidas necessárias, como por exemplo apresentação gráfica ou notificação de contactos.

Um destes *plugins*, o check_cisco_ip_sla [30], permite a obtenção de valores de operações IP SLA configuradas num equipamento Cisco. Não permite a sua configuração automática, mas testa todas as operações IP SLA configuradas no equipamento retornando um output semelhante ao output obtido por consola.

3.3.2 *Cacti*

O *Cacti* [31], *tal como indicado em* [32] é uma ferramenta o*pen source* para monitorização de redes. Para poder ser utilizado necessita que o sistema tenha instalado *RRDTool*, o sistema de *Structured Query Language* (SQL) *MySQL*, *HyperText Preprocessor* (PHP) e um servidor Web como, por exemplo, o Apache, e pode ser instalada quer em ambientes Unix quer em ambientes *Windows*.

Os seus pontos fortes passam pela facilidade de configuração, ter uma interface Web flexível, ter um fórum público com uma comunidade bastante activa, o que permite a introdução de novas funcionalidades e melhoramentos, partilha de templates entre utilizadores e a integração com outras ferramentas como o NTOP.

A partir da interface gráfica do *Cacti* é possível fazer todas as suas configurações e toda a gestão da monitorização da rede e a obtenção de dados é feita utilizando uma ferramenta denominada *Poller* que é executada a partir do programa responsável pelo agendamento de operações num sistema operativo, em Unix o *crontab*. Para obter dados o *Cacti* usa o SNMP, podendo monitorizar todos os equipamentos que o utilizam. Para o armazenamento dos dados o *Cacti* utiliza o *RRDTool*. O *Round Robin Database* (RRD) é um sistema que permite armazenar e apresentar dados graficamente baseada no *RRDTool* na sua função de criação de gráficos que combinada com o servidor Web permite que os gráficos criados sejam acedidos a partir de um qualquer browser ou plataforma.

O que distingue o *Cacti* dos demais é a utilização de templates. Estes templates permitem facilitar a configuração de recolha de dados, sem que para isso interesse o equipamento que os irá disponibilizar.

O *Cacti* possuí templates para recolha de dados de operações Cisco IP SLA, que podem ser encontradas em [33], tais como HTTP, DNS, ICMP, UDP, FTP e DHCP, sendo necessário importar as MIBs IP SLA da Cisco para a sua recolha. O utilizador também tem de configurar as operações por CLI e habilitar a permissão de acesso por SNMP ao equipamento. Estes templates permitem a recolha de dados e a sua posterior apresentação gráfica.

3.3.3 *Zenoss*

O *Zenoss Core* [34], tal como indicado em [35] é uma aplicação *open source* de gestão de redes e servidores lançado sobre a licença GNU GPL versão 2 que fornece uma interface Web para administração de sistema, monitorização de disponibilidade, desempenho e eventos. Possuem uma versão empresarial, paga, baseada na versão Core, no entanto existe uma comunidade bastante activa do *Zenoss* que desenvolve novas funcionalidades, documentação, manuais e fóruns de discussão para a versão gratuita o que permite que o *Zenoss* esteja sempre a evoluir com novas soluções e serviços.

O *Zenoss* é baseado, não só em programação própria baseada na linguagem de programação *Python*, mas também através da integração de tecnologias open source, como o *MySQL* para base de dados, *RRDTool* para ferramenta de suporte gráfico, o NET-SNMP para suporte SNMP para monitorização de informações de sistema, o Framework de rede *open source Twisted*, para a criação de servidores *Secure Shell* (SSH), proxy, HTTP e SMTP e o servidor de aplicações *Zope*.

Tal como em outras ferramentas, a partir da interface gráfica é possível gerir realizar a gestão de sistema e também tem suporte para o formato de *plugins* do *Nagios*, a que dão o nome de *Zen Packs*, [36], que são usados para adicionar novas funcionalidades para aumentar as funcionalidades e capacidades do Zenoss.

Possuí um *Zen Pack*, o Cisco IP SLA, que pode ser encontrado em [37], que apesar de ser antigo e não possuir, mesmo nos fóruns da *Zenoss*, muitas informações permite a recolha e monitorização de dados das operações Cisco IP SLA, mas não a configuração automática de operações, nem a geração de alertas ou notificações.

3.3.4 *OpenNMS*

O *Open Network Management System* (NMS) [38], é uma plataforma *open source* de gestão e monitorização de redes empresariais. Desenvolvida sob o modelo de gestão de redes *Fault, Configuration, Accounting, Performance and Security* (FCAPS) é distribuída sobre a licença GPL.

O *OpenNMS* tal como indicado em [39], é escrito em Java, para além de utilizar para base de dados o *PostgreSQL* e o *RRDTool*, mais concretamente o *JRobin* (porta Java para o *RRDTool*), para ferramenta gráfica e tem suporte para diversos sistemas operativos.

As suas funcionalidades passam pela determinação de disponibilidade e latência de serviços, recolha, armazenamento e apresentação de dados recolhidos, gestão de eventos (como por exemplo SNMP *traps*), alarmes e notificações.

O *OpenNMS* possuí um *plugin*, o Cisco IP SLA Monitor que pode ser encontrado em [40], que permite monitorizar as configurações IP SLA existentes em equipamentos Cisco. Para tal é necessário configurar as operações no equipamento introduzindo valores de *timeout*, *threshold* e *tag* e configurar o *OpenNMS* para detecção automática e monitorização das operações. Possuí duas formas de monitorizar a disponibilidade de uma operação IP SLA, uma tendo em conta o valor de *timeout*, em que o serviço é dado como em baixo se o seu valor for alcançado, outro tendo em conta o valor de *threshold*, em que o serviço é dado como em baixo se o valor for ultrapassado.

Possuí também o Cisco IP SLA *Support*, que permite a recolha de dados das operações para posterior visualização e notificação. Tal como no *plugin* anterior é necessário configurar as operações no equipamento, mas também adicionar as *Object Identifier* (OID) das Cisco RTTMON-MIB para recolha de dados e configurar o *OpenNMS* para criação e apresentação dos gráficos dos dados recolhidos, tal como apresentado em [41].

3.4 Conclusões

Analisando as ferramentas apresentadas concluí-se que todas elas em matéria de SLAs utilizam a tecnologia Cisco IOS IP SLA para a monitorização de SLAs.

Enquanto as ferramentas comerciais, para além da visualização de estatísticas de desempenho das diversas métricas, permitem a configuração remota de operações, detecção automática de equipamentos, bem como o envio de alertas e notificações de acordo com os valores obtidos, podendo desta forma ser consideradas ferramentas de gestão de SLAs, já as ferramentas *open source* estão limitadas à recolha e visualização de dados de operação, não tendo por isso todas as características e funcionalidades necessárias para serem consideradas ferramentas de gestão de SLAs, mas sim ferramentas meramente de monitorização de métricas associadas a um SLA.

Como tal fica demonstrado que o objectivo de desenvolver uma ferramenta *open source* direccionada para a monitorização e gestão de SLAs de uma rede empresarial é algo de útil e necessário, podendo desta forma reduzir os custos inerentes a um contrato de SLA.

Capítulo 4

Caracterização e Implementação do sistema

Neste capítulo é efectuada a caracterização do sistema para uma interface Web de monitorização IP SLA, bem uma a descrição da implementação da solução concretizada.

4.1 Caracterização do sistema

4.1.1 Requisitos Funcionais

Na avaliação funcional de uma interface Web de monitorização de IP SLAs deve-se apontar as capacidades da solução, deste modo, a solução deveria ter a capacidade de:

- Aproveitamento da tecnologia Cisco IOS IP SLA;
- Configuração remota automática de operações IP SLA;
- Recolha e visualização dos dados da operações;
- Monitorização simultânea de múltiplas operações em múltiplos equipamentos;
- Especificação de contratos, introduzindo informação sobre métricas, valores e penalizações contratadas;
- Associação de operações SLA a métricas definidas num contrato SLA;
- Apresentação de alertas e eventos do sistema;
- Envio de notificações, no caso relatórios por *email*.

4.1.2 Requisitos de desempenho

Para a avaliação de desempenho da interface Web de monitorização é também necessário avaliar os requisitos do servidor a utilizar. Na escolha do servidor deve ter sido em conta:

- Capacidade de processamento: Deverá ser capaz de suportar o processamento de uma interface Web em PHP, com necessidade de visualização de dados que para períodos de tempo mais altos, por exemplo 1 ano, pode levar à apresentação de mais de 100 mil registos;
- Capacidade de armazenamento: Deverá permitir a recolha e armazenamento de centenas de milhares de registos tendo como base a possibilidade de recolha de vários tipos de métricas.

4.1.3 Métricas a monitorizar

Tendo em conta uma análise efectuada sobre o tipo de contratos existentes no mercado verificou-se que as principais métricas num contrato SLA são a disponibilidade, a latência e a perda de pacotes.

A partir desta informação a operação IP SLA utilizada num equipamento Cisco para verificação de latência e disponibilidade entre dois pontos de rede é a ICMP-Echo, pelo que foi essa a principal operação implementada na interface Web. Como já foi apresentado no capítulo 3.1.1, a partir desta operação não se obtêm os valores de perda de pacotes pelo que foi necessária a criação de scripts *shell* para recolha de valores para esta métrica aquando da configuração de operações ICMP-Echo.

Para além da configuração desta operação também foi possível disponibilizar a configuração de operações DNS, DHCP e HTTP devido às semelhanças nos seus parâmetros de configuração em relação à operação ICMP-Echo e o tipo de resultados obtido ser idêntico.

4.1.4 Escolhas tecnológicas

4.1.4.1 Interface Web

A interface foi desenvolvida com recurso a várias ferramentas de software de domínio público. A linguagem escolhida para o seu desenvolvimento da foi o PHP [42], pela sua extensa biblioteca de funções assim como pela capacidade de programação orientada a objectos.

Além do uso de PHP para desenvolver a interface visual da página *Web* e para troca de dados entre a mesma e a base de dados, foi usado *jquery* [43], *jqueryUI* [44] e *javascript* [45] para menus e outras animações tais como tabelas e formulários.

4.1.4.2 Servidor base de dados

Para servidor de base de dados foi feita uma ponderação entre o *PostgreSQL* e o MySQL [46], pois são dos servidores de base de dados mais utilizados devido à sua robustez, fiabilidade e desempenho, são *open source e* possuem um grande suporte da comunidade quer ao nível de documentação, manuais ou fóruns de discussão.

Foi escolhido o MySQL uma vez que nunca tinha trabalhado com este tipo de sistema e considerei que a sua utilização seria uma mais-valia em termos de conhecimento e também porque permite que os dados armazenados possam ser usados por outras aplicações e permite também efectuar análise de dados directamente da base de dados.

4.1.4.3 Recolha de dados

Para a recolha de dados utilizaram-se *scripts shell*, tanto para recolha de dados de operações IP SLA, como para teste de perda de pacotes, sendo que os scripts de recolha de dados dos equipamentos Cisco, faziam essa recolha por SNMP v2. Cada script era executado de 5 minutos em 5 minutos.

4.1.4.4 Ferramenta Gráfica

A ferramenta que permitiu o desenho gráfico dos valores obtidos dos testes, é designada de *RGraph*¸ que pode ser encontrada em [47]. O *RGraph* é uma biblioteca gráfica em HML5 que usa a *tag canvas* do HTML5 para realizar diversos tipos de gráficos. Além de criar gráficos, permite ao utilizador visualizar pontos específicos dos gráficos ao passar com o rato por cima do mesmo, fazer zoom no mesmo, entre outras.

Foi usada a versão *stable* de 25 de Março de 2011 e tipo de gráfico usado foi um *line chart*. Para a realização do gráfico é necessário colocar no HTML a *tag*

<canvas id="myCanvasTag" width="1000" height="400";>[No canvas support]</canvas>

4.1.4.5 Configuração de operações

Para a configuração das operações nos equipamentos a partir da interface Web foi utilizado o script PHP-Telnet [48], que permite executar sessões telnet a partir de scripts PHP. Também foi utilizado este script para executar comandos no servidor onde corria a interface Web que necessitavam de permissões de *root*.

4.1.4.6 Script de recolha de dados de operações IP SLA

Para recolha dos dados obtidos, num equipamento Cisco, de operações IP SLA foram criados scripts *shell*. As acções realizadas foram a da recolha por SNMP de valor para uma variável, inserir o valor da variável na base de dados, inserir evento na base de dados e verificar valor da variável e envio de alerta se a variável estiver vazia, se o valor da variável for igual a zero, se o valor da variável ultrapassar o limite da métrica associada e se o valor da variável indicar que a operação IP SLA não se encontrava configurada.

```
#!/bin/bash

id=id teste sla base de dados
idcontrato=id contrato base de dados
idevent=3
information="Value for test sla id associated to contract id idcontrato inserted in database"
valor=`snmpget -v2c -c public ip_equipamento 1.3.6.1.4.1.9.9.42.1.2.10.1.1.id | awk '{print $4}'`
echo
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO teste (idsla, data, valor) VALUES ('$id', NOW(), '$valor');"
echo
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO events (date_time, ideventtype, information, idcontrato) VALUES (NOW(), '$idevent', '$information', '$idcontrato');"
echo
if [ -z "$valor" ]
then
idalert=3
status="CRITICAL"
description="Loss of connectivity to ip_equipamento "
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO alerts (date_time, idalerttype, infostatus, description, idcontrato) VALUES (NOW(), '$idalert', '$status', '$description', '$idcontrato');"
fi
if [ "$valor" -eq 0 ]
then
idalert=2
status="CRITICAL"
description="Value for sla teste id in contract id idcontrato is NULL"
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO alerts (date_time, idalerttype, infostatus, description, idcontrato) VALUES (NOW(), '$idalert', '$status', '$description', '$idcontrato');"
```

```
secidalert=4
status="CRITICAL"
description="Loss of connectivity to destiny ip_destino"
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO
alerts (date_time, idalerttype, infostatus, description, idcontrato) VALUES (NOW(),
'$idalert', '$status', '$description', '$idcontrato');"
fi
if [ "$valor" -gt 10 ]
then
idalert=2
status="WARNING"
description="Value for sla teste id in contract id idcontrato EXCEEDED the limit"
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO
alerts (date_time, idalerttype, infostatus, description, idcontrato) VALUES (NOW(),
'$idalert', '$status', '$description', '$idcontrato');"
fi
if [ "$valor" = "Such" ]
then
idalert=5
status="CRITICAL"
description="Sla test id NOT CONFIGURATED in ip_equipamento"
mysql --host=localhost --user=root --password=root --database=my_db -e "INSERT INTO
alerts (date_time, idalerttype, infostatus, description, idcontrato) VALUES (NOW(),
'$idalert', '$status', '$description', '$idcontrato');"
fi
echo
```

Figura 4.1 – Script de recolha de dados por SNMP

4.1.4.7 Script para teste de perda de pacotes

Para recolha dos dados de perda de pacotes foram criados scripts *shell*. As acções realizadas foram realizar teste ping ao IP de destino, colocar valor do resultado numa variável, inserir valor da variável na base de dados, inserir evento na base de dados, verificar valor da variável e envio de alerta em caso do valor diferente de zero.

```
#!/bin/bash

id=id teste sla base de dados
idcontrato=id contrato base de dados
idevent=3
valor=`ping -c npacotes ip_destino | awk '/%/ {print $6}' | cut -d% -f1`
echo
if [ "$valor" -eq 0 ]
then
information="Value for packet loss for ip_destino associated to contract id inserted in database"
echo
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO pack_loss (idsla, data, loss) VALUES ('$id', NOW(), '$valor');"
echo
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO events (date_time, ideventtype, information, idcontrato) VALUES (NOW(), '$idevent', '$information', '$idcontrato');"
echo
fi
if [ "$valor" -ne 0 ]
then
ping=`ping -c npacotes ip_destino | awk '/%/ {print $8}' | cut -d% -f1`
information="Value for packet loss for ip_destino associated to contract id inserted in database"
echo
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO pack_loss (idsla, data, loss) VALUES ('$id', NOW(), '$ping');"
echo
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO events (date_time, ideventtype, information, idcontrato) VALUES (NOW(), '$idevent', '$information', '$idcontrato');"
echo
if [ "$ping" -ne 100 ]
then
idalert=1
status="WARNING"
description="Value for % of packet loss for ip_destino associated to contract id is  NOT NULL"
echo
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO alerts (date_time, idalerttype, infostatus, description, idcontrato) VALUES (NOW(), '$idalert', '$status', '$description', '$idcontrato');"
fi
```

```
if [ "$ping" -eq 100 ]
then
idalert=1
status="CRITICAL"
description="Value for % of packet loss for ip_destino associated to contract id is  100 %"
echo
mysql --host=localhost --user=### --password=### --database=my_db -e "INSERT INTO alerts (date_time, idalerttype, infostatus, description, idcontrato) VALUES (NOW(), '$idalert', '$status', '$description', '$idcontrato');"
fi
fi
```

Figura 4.2 – Script para recolha de dados de perda de pacotes

O funcionamento dos scripts é ilustrado na figura 4.1

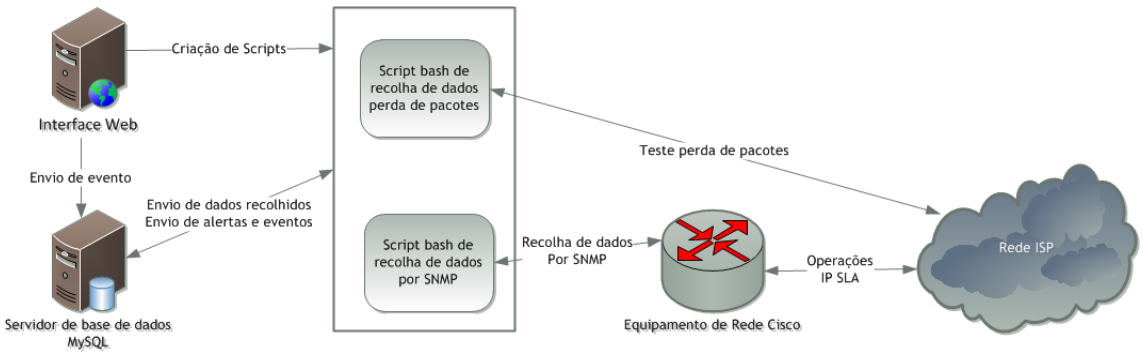


Figura 4.3 – Funcionamento de scripts

4.1.4.8 Notificações

Para o envio de notificações criou-se 3 scripts PHP, para três situações distintas:

- *mail*.php: Verificava último valor de latência na base de dados para cada um dos testes configurados e caso esse valor fosse igual a zero corria uma função para envio de emails que testa se o servidor tem conectividade com o equipamento Cisco. Neste caso pode enviar dois tipos de emails, perda de conectividade com o equipamento e perda de conectividade com o IP de destino. Caso o valor ultrapasse o limite, executa outra função que envia um *email* de valor de métrica ultrapassado. Executado a cada 5 minutos;
- *mail_loss*.php: Verificava último valor na base de dados para perda de pacotes associado a cada um dos testes configurados. Caso esse valor não fosse igual a zero enviava *email* a indicar perda de pacotes no teste. Executado a cada 5 minutos;

- *mail_report*.php: Retira da base de dados valores de máximo, mínimo e média de latência e perda de pacotes, bem como períodos de indisponibilidade de serviço para cada um dos testes configurados, enviando *email* com essa informação. Executado uma vez por mês.

Na Figura 4.4 é apresentado o seu funcionamento.

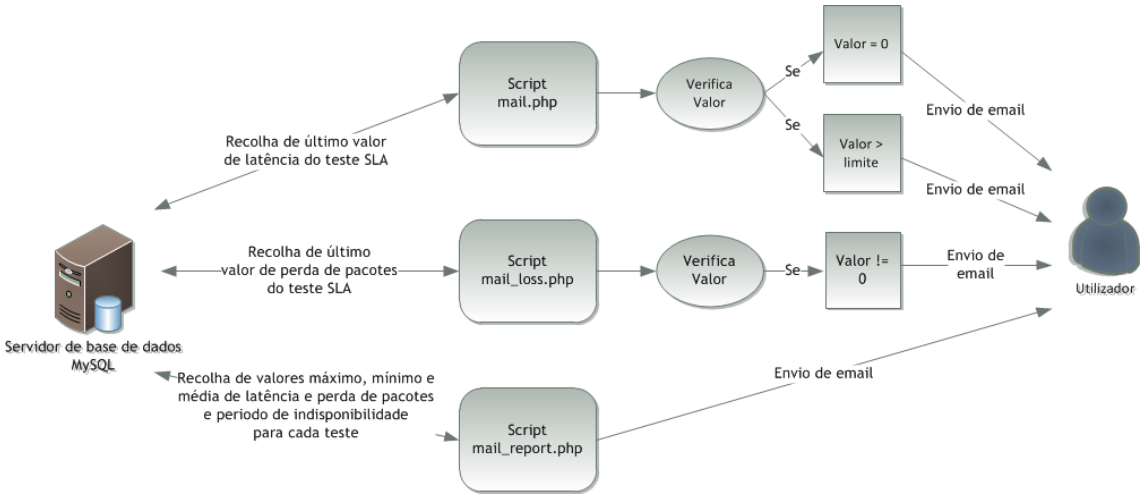


Figura 4.4 – Funcionamento de scripts de envio de emails

4.2 Implementação do sistema

Resumindo, a principal tecnologia *open source* integrada foi em termos de sistema Operativo o *Debian* 5.05 (*Lenny*) [49], para servidor Web o Apache2 [50], a linguagem de desenvolvimento interface Web foi o PHP, com a recolha de dados a ser feita por SNMP e pela utilização da ferramenta *RGraph* para suporte gráfico dos dados.

Em termos de interface Web, ela deviria permitir funções de acesso e gestão de sistema através de configuração de contratos, configuração de testes SLA associados a contratos, visualização gráfica de dados de estado e desempenho dos teste, autenticação de utilizadores, configuração e visualização de eventos, alertas e notificações via *email*.

Em termos de base de dados ela devia armazenar dados de sistema e serviços recolhidos para apresentação, dados de configurações de sistema (equipamentos, utilizadores, serviços) e dados de eventos, alertas e notificações.

As métricas e operações a monitorizar foram a operação ICMP-*Echo* através da medição de RTT a um IP de destino e a perda de pacotes a um IP de destino através de um teste de conectividade (*ping*).

4.2.1 Configurações

Para a interface gráfica, foi então instalado no servidor a correr as aplicações já referidas no capítulo 4.2, além de um sistema de base de dados *MySQL,* onde eram armazenados os dados medidos, os registos usados, parâmetros das configurações e a conta de utilizador para efectuar o login na página *Web*.

Para a interface gráfica poder realizar o conjunto de operações pretendidas também se teve de instalar os pacotes *snmp* para recolha de dados, telnet para aceder remotamente aos equipamentos Cisco, *telnetd* para a interface Web poder aceder à máquina local, *sendmail-bi*n e *sendmail*: para o envio de emails e *fping* que foi a ferramenta usada para verificar conectividade aos equipamentos nos scripts de *email*.

Após a instalação dos diversos pacotes, renomeou-se o ficheiro */etc/securetty* criado pelo pacote *telnetd* para */etc/securetty.bak* de forma a permitir o acesso por telnet à máquina local ao utilizador *root*, tal como descrito em [51].

Criou-se a pasta */root/scripts/* para a colocação aí dos scripts criados pela interface Web, precisando mudar as suas permissões, tal como a pasta */etc/cron.d*.

Como se instalou o Apache2 e a sua pasta por defeito é a pasta */var/www/* colocou-se aí a interface Web desenvolvida, copiando-se de seguida o ficheiro *sla_mail* para a pasta */etc/cron.d/* reiniciando-se de seguida o *cron*.

O ficheiro *sla_mail* é um ficheiro de *crontab* de forma a permitir a execução dos scripts de *email* nos intervalos de tempo indicados no capítulo 4.1.4.8. O seu conteúdo foi o seguinte

```
*/5 * * * * root lynx -dump http://localhost/tese/mail.php
*/5 * * * * root lynx -dump http://localhost/tese/mail_loss.php
0 0 1 * * root lynx -dump http://localhost/tese/mail_report.php
```

Figura 4.5 – Ficheiro *crontab* para envio de *emails*

4.2.2 Base de dados

Tal como escrito anteriormente, a base de dados utilizada na realização deste trabalho foi o *MySQL*. Para a administração da base de dados utilizou-se o *phpmyadmin* [52], uma ferramenta Web escrita em PHP para gestão de base de dados.

O esquema da base de dados utilizada neste trabalho é apresentado na Figura 4.6.

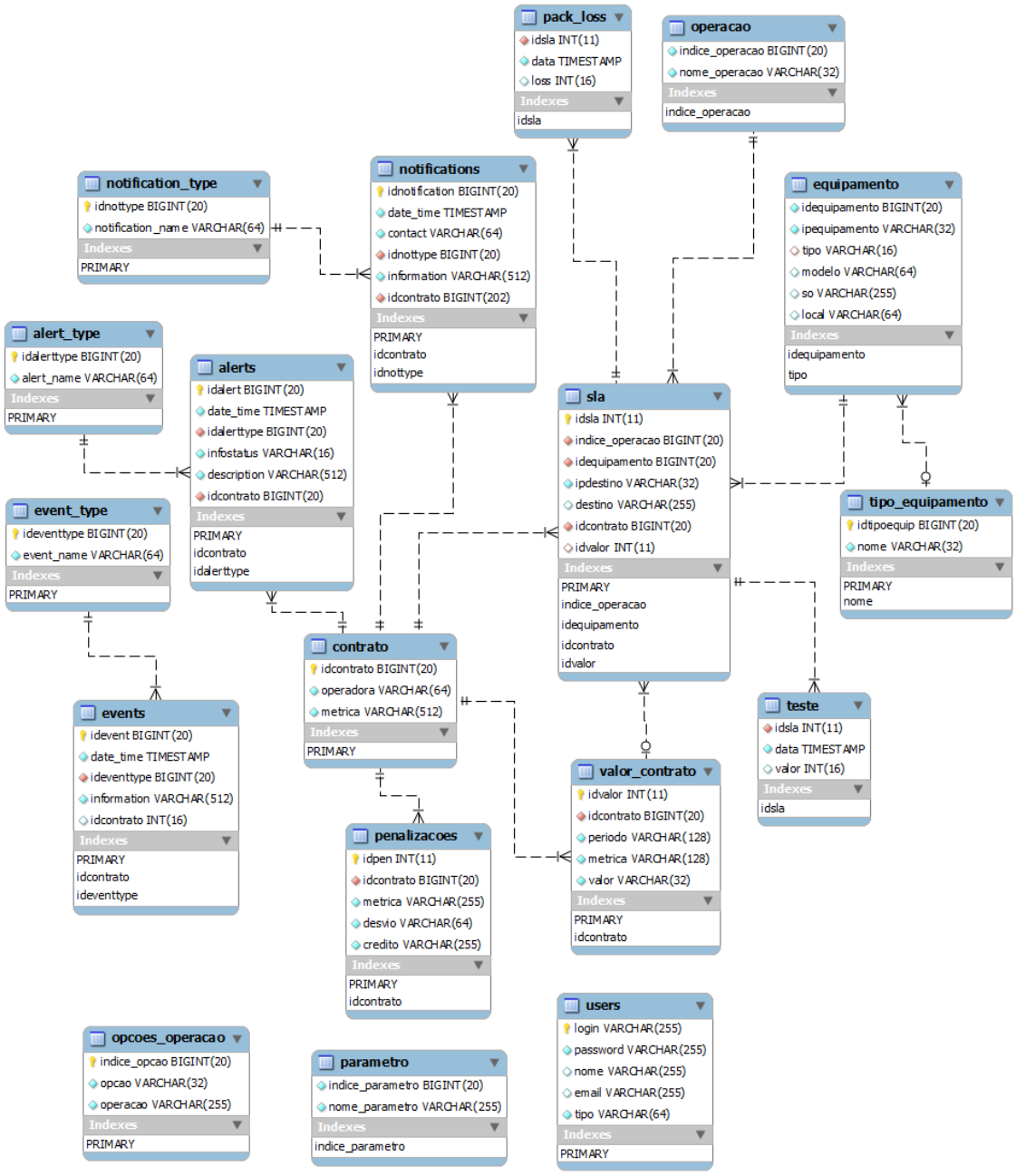


Figura 4.6 - Esquema base de dados do sistema

A tabela contrato é o ponto central da base de dados e nela foi guardada a informação genérica do contrato SLA enquanto nas tabelas penalizações e valor_contrato são guardadas as informações específicas, tendo como chave estrangeira o índice do contrato associado. A tabela operação guarda a informação sobre as operações que podem ser configuradas, a tabela equipamento guarda a informação dos equipamentos onde os testes são efectuados, enquanto a tabela sla guarda a informação dos testes criados na interface Web, tendo chaves estrangeiras indicativas da operação executada, do equipamento onde se realiza o teste, o contrato e valores associados ao teste. As tabelas *pack_loss* e teste guardam os valores

obtidos para perda de pacotes e latência, respectivamente, tendo uma chave estrangeira indicativa do teste a que está associado.

As tabelas *event_type*, *alert_type*, *notification_type* guardam a informação sobre o tipo de eventos, alertas e notificações que o sistema pode gerar. As tabelas *alerts* e *notifications* guardam a informação relativa aos alertas e notificações criados pelo sistema, tendo chaves estrangeiras indicativas do contrato associado e do tipo de alertas e notificações. Já a tabela *events* que guarda a informação dos eventos criados pelo sistema só possuí chave estrangeira ao tipo de evento, apesar de um dos seus parâmetros ser o índice de contrato associado, tal acontece por haver tipos de eventos sem associação a contratos.

A tabela *users* guarda a informação do utilizador com acesso à interface Web, enquanto as tabelas parâmetro e opções_operação guardam informação relativa a comandos e parâmetros de configuração de operações, sendo usadas meramente para apresentação dessa informação na interface Web.

4.2.3 Interface Web

A interface Web desenvolvida permitiu introduzir informação relativa a contratos SLA assinados pelo utilizador, podendo indicar métricas, valores e penalizações contratadas. A partir dela pôde-se criar, editar e pagar testes SLA associando-os a contratos e métricas já existentes de forma a recolher dados que permitiam a sua monitorização e a observação dos dados recolhidos graficamente ou em tabela. Também possuía um registo com evento, alertas e notificações que ocorreram no sistema.

Antes de aceder à interface Web, era pedido inicialmente ao utilizador que efectua-se login tal como apresentado na Figura 4.7

Figura 4.7 - Interface Web: Autenticação

Após a autenticação aparecia uma página de boas vindas, como se mostra na Figura 4.8 com um menu lateral com diversas opções. Caso já possuí-se na base de dados informação sobre algum contrato também aparecia a lista de contratos.

Figura 4.8 – Interface Web: Página Inicial

Seguindo o menu Configuração -> Contratos, aparecia uma nova página onde se podia inserir, editar e apagar informação referente a contratos assinados. Neste ponto apenas informação sobre operadora e métricas contratadas era pedida, tal como apresentado na Figura 4.9.

Figura 4.9 – Interface Web: Página de contratos

Depois associava-se a cada contrato os valores contratados seguindo a opção Configuração -> Valores Contrato. Começava-se por associar esse valor a um contrato existente na base de dados e depois introduzir informação relativa a período, métrica e valor, tal como apresentado na Figura 4.10.

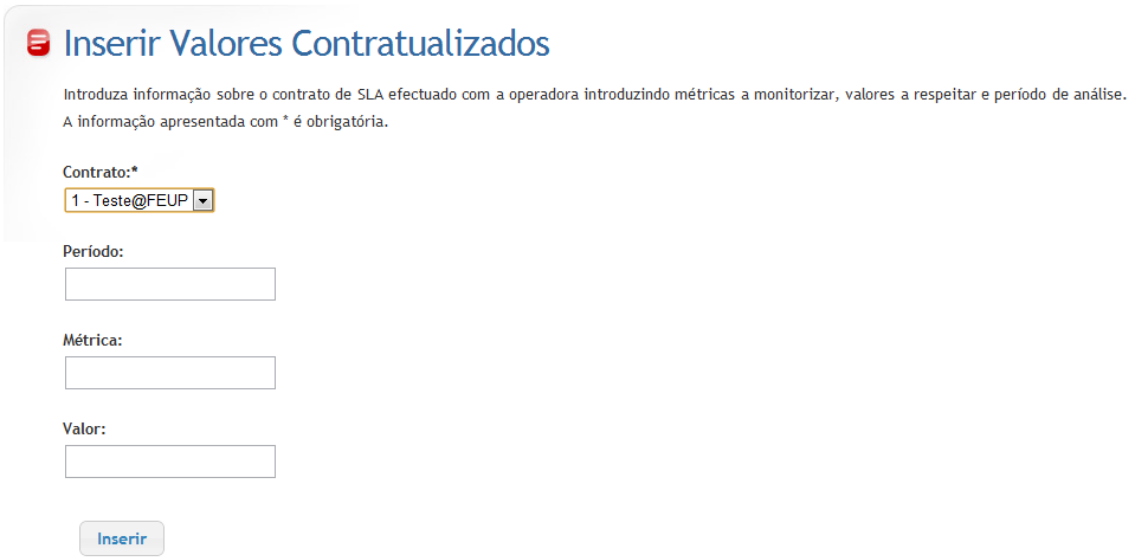


Figura 4.10 – Interface Web: Inserir valores de contrato

Também se pôde introduzir a informação sobre as penalizações contratadas para cada métrica em caso de incumprimento do SLA. Seguindo no menu a opção Configuração -> Penalizações pôde-se introduzir essa informação associando-a a um contrato e a uma métrica desse contrato, indicando qual o desvio e valor do crédito acordado, tal como apresentado na Figura 4.11.

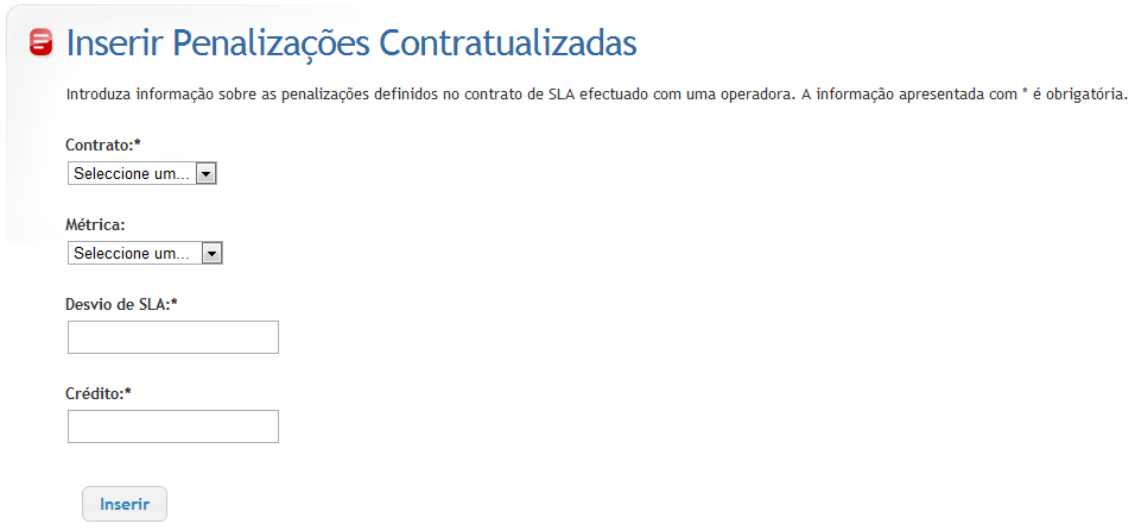


Figura 4.11 – Interface Web: Inserir penalizações de contrato

Depois de introduzir toda a informação sobre o contrato SLA, na página inicial da interface aparecia a lista de contratos existente na base de dados, podendo-se consultar toda a informação introduzida na opção Detalhes.

Para se proceder à configuração de testes para verificação do cumprimento dos SLA devia-se primeiro introduzir a informação sobre o equipamento Cisco onde se pretendia configurar as operações IP SLA, seguindo o menu na opção Configuração -> Equipamentos. Tal como apresentado na Figura 4.12 devia-se introduzir obrigatoriamente o IP da interface onde se pretendia realizar o teste e depois um conjunto de informações que passavam pelo tipo de equipamento que era (router ou *switch*), modelo do equipamento, sistema operativo que usava e local onde se encontrava, tal como apresentado na figura, sendo que esta informação não era obrigatória, mas servia para uma melhor compreensão.

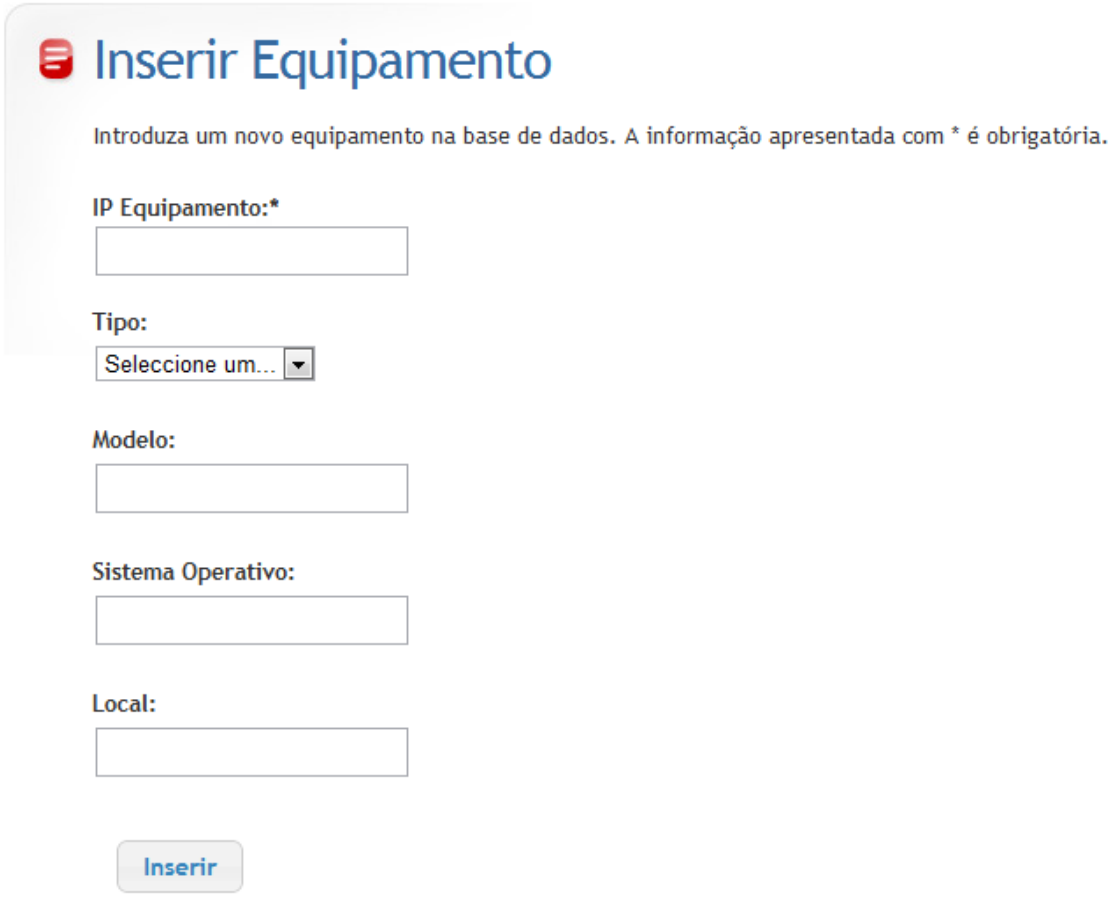


Figura 4.12 – Interface Web: Inserir Equipamento

Deste modo podia-se criar os testes SLA para recolha de dados para monitorização, ao escolher no menu a opção Configuração -> Teste SLA.

Aí configurava-se o teste, tal como é apresentado na Figura 4.13, indicando a que contrato e métrica devia ser associado, indicando um identificador para esse teste, um número inteiro entre 1 e 2147483647, tal como especificado no comando Cisco para configuração de uma operação SLA. Indicava-se como IP de origem um dos IPs da interface de equipamento introduzidos na base de dados e qual a operação pretendida para o teste, estando disponíveis as opções *ICMP-echo*, HTTP, DNS e DHCP.

De seguida introduzia-se a informação sobre o IP de destino do teste e nome associado a esse destino, frequência e número de pacotes para a realização do teste de perda de pacotes. Finalmente introduzia-se as credenciais de acesso ao equipamento Cisco onde se ia realizar o teste, as credenciais de acesso à base de dados do sistema e as credenciais de acesso *root* à máquina onde a interface Web estava a correr.

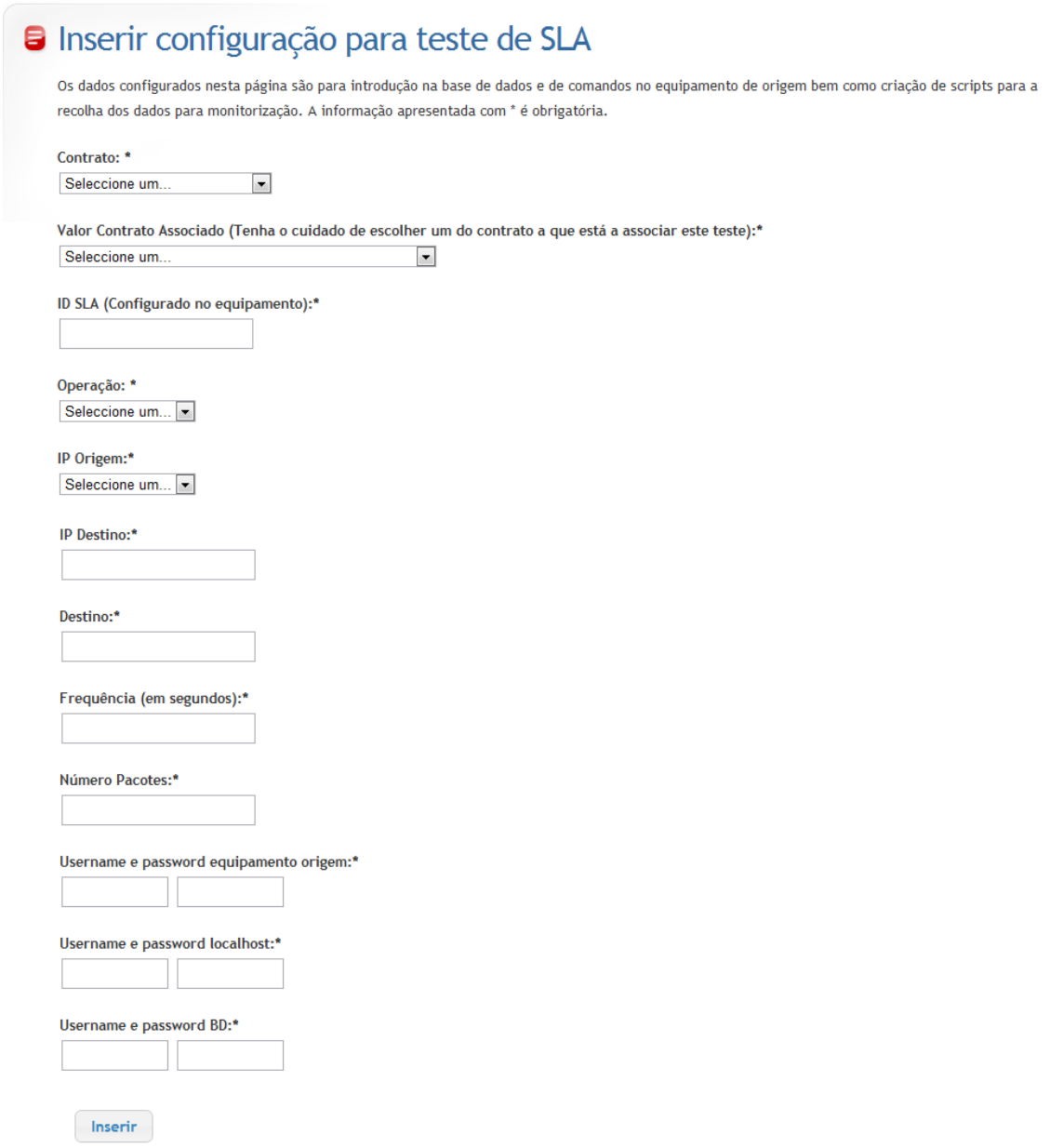


Figura 4.13 – Configuração de teste SLA

Depois de se introduzir toda esta informação eram realizadas as diferentes tarefas, envio automático de comandos para o equipamento Cisco, criação de script para recolha de dados desse teste, criação de script para teste de perda de pacotes, criação de ficheiros de *crontab* para execução periódica dos scripts e reinício do *crontab* do sistema.

A partir da interface Web também se podia observar o histórico de eventos que ocorreram no sistema, podendo-se escolher observar todos os eventos, ou eventos específicos associados a um contrato ou sem associação a contratos.

Os eventos encontravam-se divididos nas seguintes categorias:

- Login: Autenticação de utilizador;
- Teste SLA: Criar, editar ou apagar testes SLA;
- Base de Dados: Inserir, editar ou remover informação na base de dados;
- Script: Criar, editar ou apagar scripts para recolha de dados.

A partir da interface Web também se pôde observar o histórico de alertas que ocorreram no sistema podendo-se escolher observar todos os alertas, ou alertas associados a um contrato.

Os alertas eram divididos nos seguintes tipos:

- Valor de Perda de Pacotes: Quando o valor obtido no teste de perda de pacotes não é zero;
- Valor de Latência: Quando o valor do teste SLA obtido por SNMP é zero ou ultrapassa o limite;
- Equipamento Inacessível: Quando o valor do teste SLA obtido por SNMP é nulo;
- Destino Inacessível: Quando o valor do teste SLA obtido por SNMP é zero;
- Teste Não Configurado: Quando o valor do teste SLA obtido por SNMP retorna *"No Such Instance currently exists at this OID"* indica que o teste com o id especificado não existe.

Os alertas também eram divididos em duas categorias:

- WARNING: Quando o valor obtido por SNMP do teste SLA ultrapassa o limite e quando o valor de perda de pacotes é superior a 0% mas inferior a 100%;
- CRITICAL: Todos os restantes casos.

Outra das funcionalidades da interface Web era permitir observar o histórico de notificações enviadas para o utilizador, podendo-se seleccionar todas as notificações ou apenas notificações associadas a um contrato específico.

As notificações estavam divididas nos seguintes tipos

- Perda de Pacotes: Envio de *email* quando o último valor obtido para perda de pacotes de um teste SLA é diferente de zero;
- Perda de conectividade com o equipamento: Envio de *email* quando o último valor obtido de um teste SLA é nulo e o teste de conectividade ao equipamento retorna que não existe conectividade com o equipamento;
- Perda de Conectividade com o destino: Envio de *email* quando o último valor obtido de um teste SLA é nulo e o teste de conectividade ao equipamento retorna que existe conectividade com o equipamento;

- Limite do teste ultrapassado: Envio de *email* quando o último valor obtido de um teste SLA ultrapassa o limite contratado com a operadora num SLA
- Relatório de Estado: Envio de *email* com relatório mensal com informações sobre valores máximos, mínimos é médias de latência e perda de pacotes e períodos de indisponibilidade para cada teste SLA.

As notificações eram enviadas a partir de três scripts PHP, de seu nome *mail*, *mail_loss* e *mail_report* sendo que utilizavam a ferramenta *fping* para teste de conectividade ao equipamento.

O *fping* retorna *"IP is alive"* caso exista conectividade ou "IP *is unreachable*" caso essa conectividade se tenha perdido.

No caso da listagem de eventos, alertas e notificações o limite máximo de itens mostrado na interface era de 300.

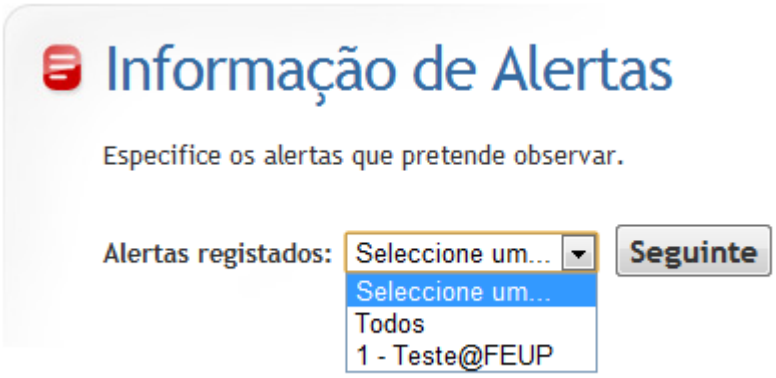


Figura 4.14 – Interface Web: Informação de alertas

Capítulo 5

Resultados

5.1 Cenário de teste

Tomou-se como cenário de teste um contrato SLA com as seguintes características.

5.1.1 Definição de métricas

Disponibilidade

A disponibilidade da conectividade IP é definida num determinado mês excluindo falhas programadas e é baseada na disponibilidade de toda a infra-estrutura IP do ISP.

Fiabilidade

Expressa por uma percentagem de pacotes que uma vez enviados para a rede IP do ISP não chegam ao seu destino enquanto transportados pelo *Backbone* IP do ISP, excluindo-se troços fora do perímetro de controlo da rede IP deste. Este efeito denomina-se por perda de pacotes.

Latência

Tempo de Trânsito ou Latência IP é definida como o período de tempo que um pacote IP demora a transitar na rede IP do ISP até chegar ao router de acesso na rede IP do ISP no ponto de saída para o seu destino. A contabilização deste atraso é expresso em milissegundos e é medido e definido unicamente para os pacotes que atingem o seu destino com fiabilidade.

5.1.2 Valores de métricas SLA

Tabela 5.1 – Valores de métricas

Métrica	Média Mensal
Disponibilidade	99,5%
Fiabilidade	Média de perda de pacotes < 1%
Latência para o *Portuguese Internet Exchange* (PIX)	20 ms
Latência para *peering* directo	10 ms
Latência para tráfego Intraeuropeu	80 ms
Latência para tráfego Transatlântico	130 ms

Janela de manutenção

O serviço de conectividade IP pode, mediante comunicação prévia, ser interrompido durante 8h por ano para manutenções na rede IP do ISP, que são maioritariamente efectuadas fora do horário laboral.

5.1.3 Penalizações

Sempre que o ISP não consiga garantir os níveis de serviço definidos anteriormente, o Cliente terá direito a uma indemnização, de valores não cumulativos prevalecendo o de maior valor até um máximo equivalente a uma assinatura mensal, calculada da seguinte forma:

Disponibilidade

Tabela 5.2 – Penalizações para a métrica disponibilidade

Desvio de SLA	Crédito
Por cada hora cumulativa de indisponibilidade de serviço	1 dia de assinatura mensal

Fiabilidade (perda de pacotes)

Tabela 5.3 – Penalizações para a métrica fiabilidade

Desvio de SLA	Crédito
Mais de 0,5 até 1%	5% da assinatura mensal
Mais de 1 até 2%	10% da assinatura mensal
Mais de 2 até 5%	15% da assinatura mensal
Mais de 5%	20% da assinatura mensal

Latência

Tabela 5.4 – Penalizações para a métrica latência

Desvio de SLA	Crédito
Mais de 1 até 5ms	5% da assinatura mensal
Mais de 5 até 10ms	10% da assinatura mensal
Mais de 10 até 20ms	15% da assinatura mensal
Mais de 20ms	20% da assinatura mensal

5.1.4 Esquema de teste

Para testar os valores de latência através da configuração da operação SLA ICMP-*Echo* utilizaram-se os valores apresentados na Tabela 5.5.

Tabela 5.5 – Associação métrica de contrato com IP de teste

Latência	IP	Destino	Localização
Peering directo	193.137.0.10	Router3.10GE.Lisboa.fccn.pt	Portugal
PIX	193.136.251.3	TelepacAS3243.gigapix.pt	Portugal
Tráfego Intraeuropeu	62.40.112.161	so-4-0-0.rt1.fra.de.geant2.net	Reino Unido
Tráfego Transatlântico	207.138.144.45	TenGigabitEthernet7-3.ar1.FRA4.gblx.net	EUA

O equipamento utilizado encontrava-se no laboratório de redes do Departamento de Engenharia Electrotécnica e de Computadores (DEEC) da Faculdade de Engenharia da Universidade do Porto (FEUP).

Tabela 5.6 – Equipamento de teste

Tipo	Sistema Operativo	IP Interface
Router Cisco 2901/K9	IOS 15.1(3)T	172.16.1.39

5.2 Resultados

Começou-se pela configuração do endereço de correio electrónico associado ao utilizador de forma a permitir o envio de *emails*.

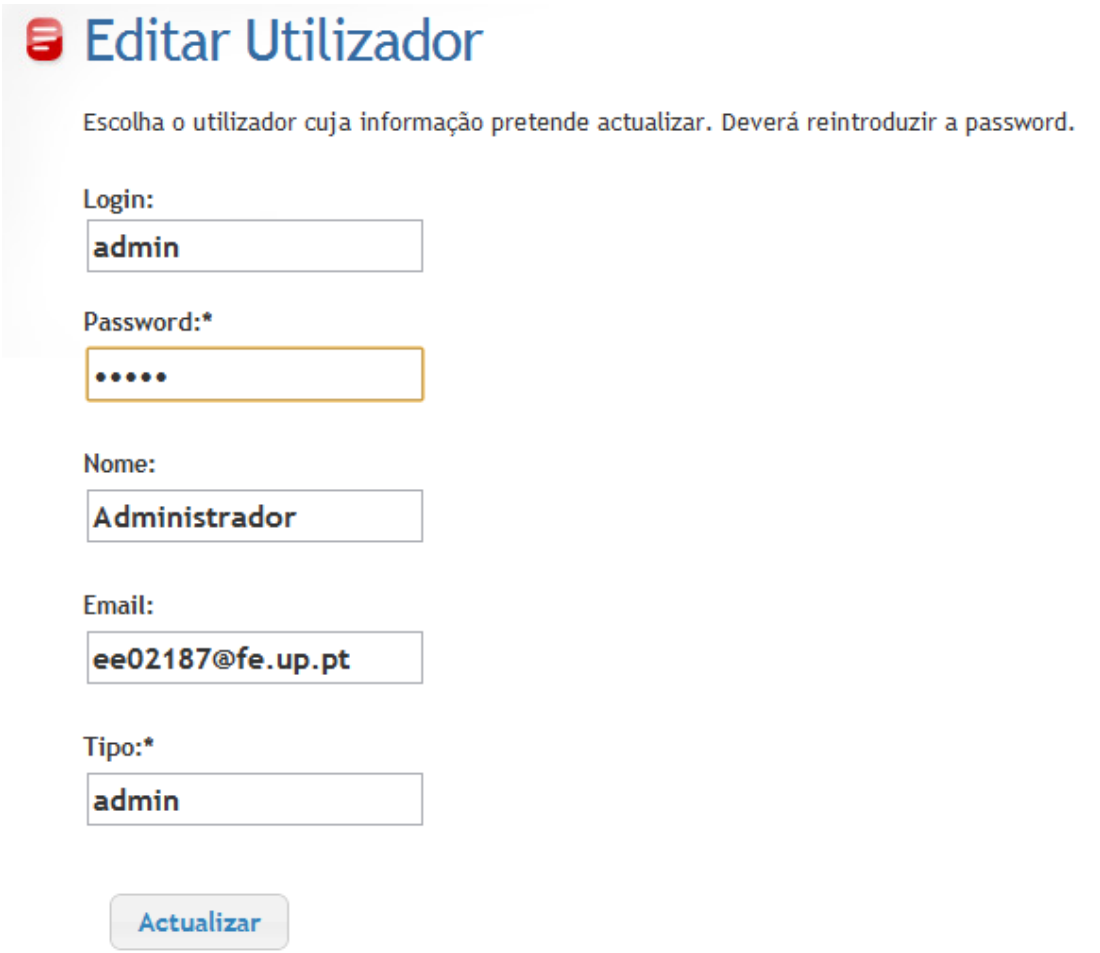


Figura 5.1 – Inserir informação de utilizador

Na interface Web foi apresentada a informação actualizada do utilizador, tal como apresentado na Figura 5.2.

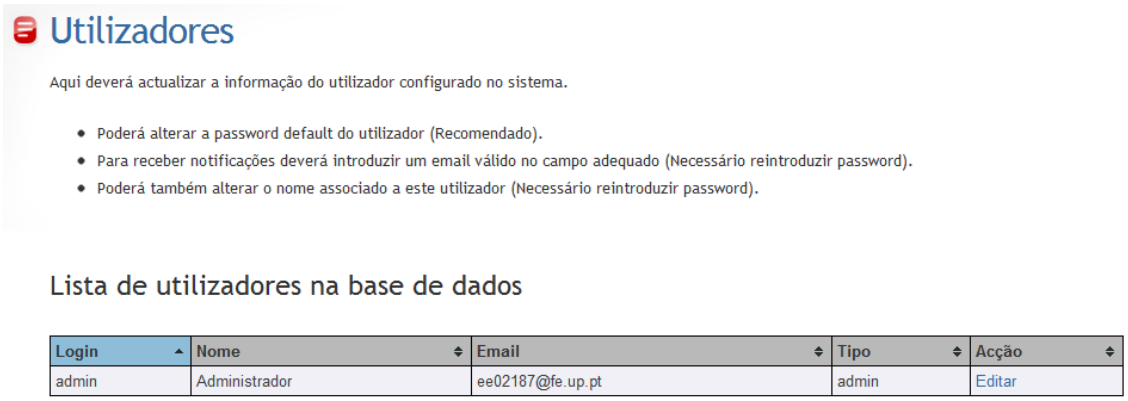


Figura 5.2 - Informação de utilizador

Seguiu-se a introdução da informação sobre o contrato de teste. Os detalhes dessa informação também são apresentados na interface tal como apresentado na Figura 5.3, Figura 5.4 e Figura 5.5.

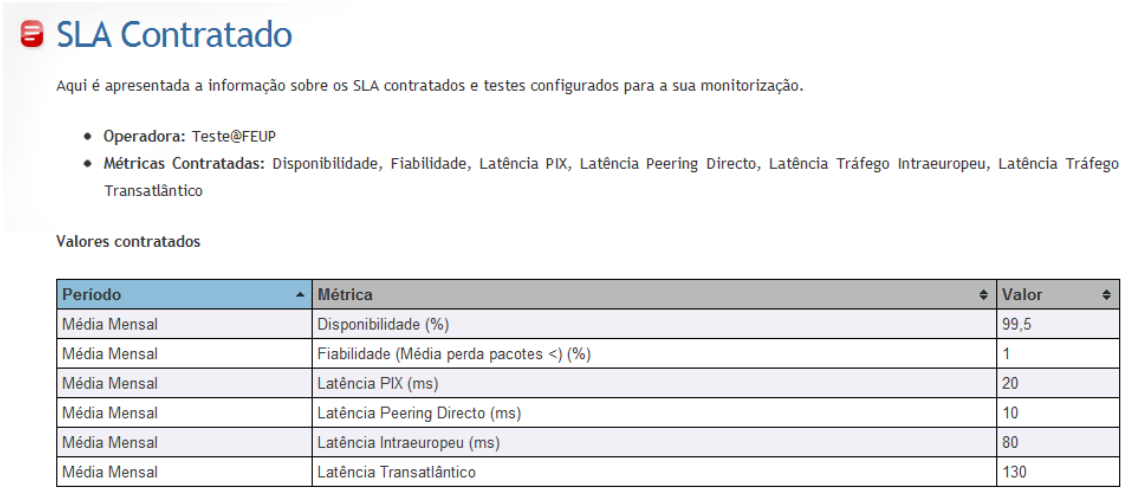


Figura 5.3 - Detalhes de contrato: valores

Penalizações Definidas

- **Disponibilidade:**

Desvio de SLA	Crédito
Por cada hora	1 dia assinatura, até máximo de 1 assinatura mensal

- **Perda de Pacotes:**

Desvio de SLA	Crédito
mais de 0,5% ate 1%	5% assinatura mensal
mais de 1% até 2%	10% assinatura mensal
mais de 2% até 5%	15% assinatura mensal
mais de 5%	20% assinatura mensal

- **Latência:**

Desvio de SLA	Crédito
mais de 1 até 5 ms	5% assinatura mensal
mais de 5 até 10 ms	10% assinatura mensal
mais de 10 até 20 ms	15% assinatura mensal
mais de 20 ms	20% assinatura mensal

Figura 5.4 – Detalhes do contrato: penalizações

Operações Configuradas

Operações configuradas no router para monitorização do SLA contratado.

ID SLA	Operação	IP Origem	IP Destino	Destino	Valor Associado
40	ICMP Echo	172.16.1.39	193.137.0.10	Router3.10GE.Lisboa.fccn.pt	Latência Peering Directo (ms)
41	ICMP Echo	172.16.1.39	193.136.251.3	TelepacAS3243.gigapix.pt	Latência PIX (ms)
42	ICMP Echo	172.16.1.39	62.40.112.161	so-4-0-0.rt1.fra.de.geant2.net	Latência Intraeuropeu (ms)
43	ICMP Echo	172.16.1.39	8.8.8.8	google-public-dns-a.google.com	Latência Transatlântico

Figura 5.5 – Detalhes do contrato: testes associados

5.2.1 Teste latência *peering* directo

A Figura 5.6 mostra a informação apresentada na página da interface Web para visualização do histórico de latência para este teste.

Figura 5.6 – Informação teste latência *perring* directo

Para melhor compreensão do padrão dos valores de latência deste teste é apresentado o histórico de um dia na Figura 5.7.

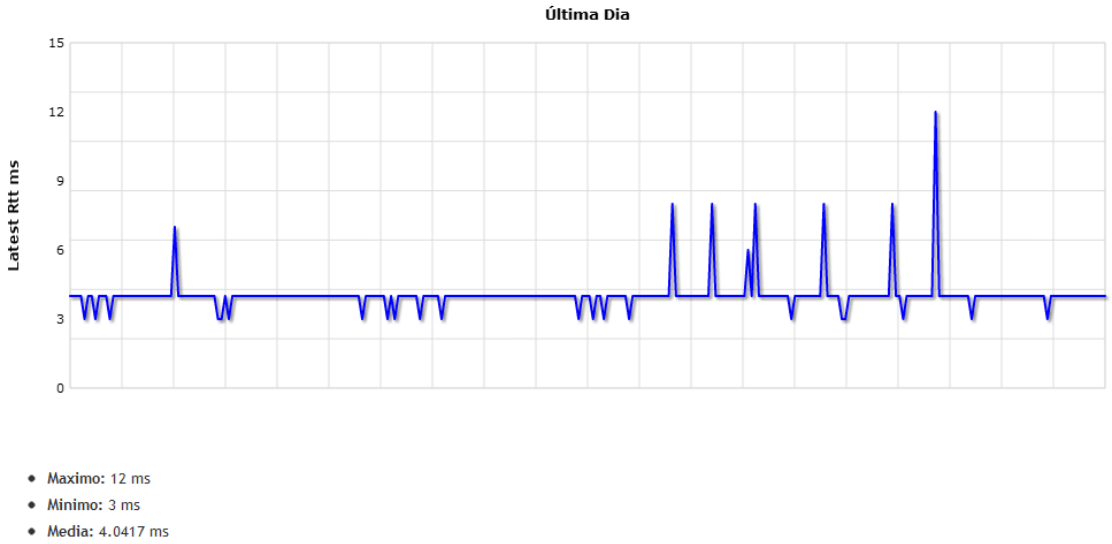


Figura 5.7 – Histórico latência *peering* directo último dia

A Figura 5.8 e a Figura 5.9 mostram o padrão de uma semana e um mês respectivamente.

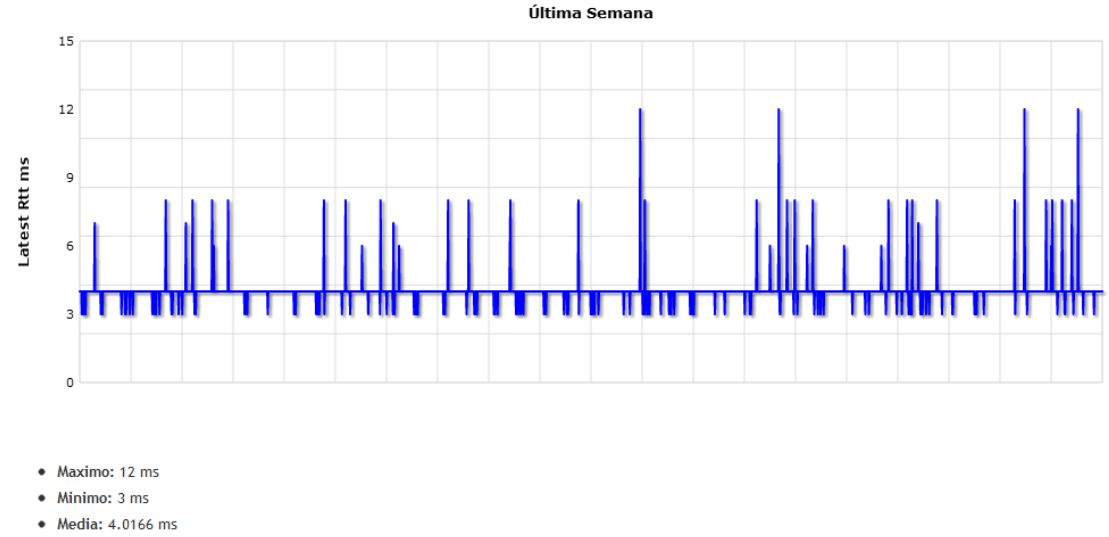


Figura 5.8 – Histórico latência *peering* directo última semana

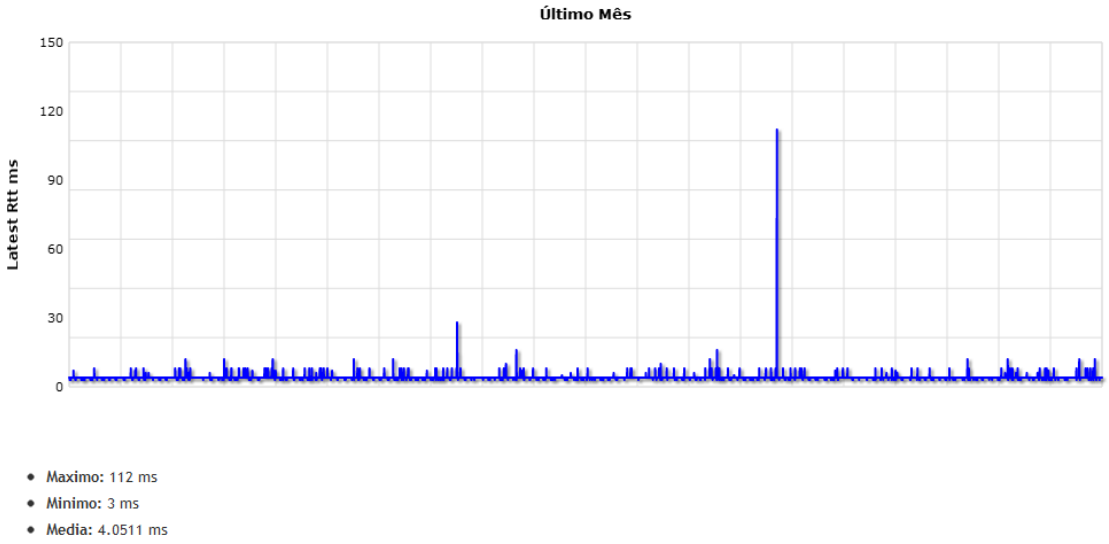


Figura 5.9 – Histórico latência *peering* directo último mês

Na Tabela 5.7 são apresentados os valores de latência máxima, mínima e média.

Tabela 5.7 – Valores latência *peering* directo

Período	Máximo (ms)	Mínimo (ms)	Média (ms)
15/05/2011 a 16/06/2011	112	3	4,0511
15/05/2011 a 02/06/2011	28	3	4,0470
02/06/2011 a 16/06/2011	112	3	4,0560

A Tabela 5.8 apresenta o número de vezes que o limite contratado para a métrica associada ao teste foi ultrapassado.

Tabela 5.8 – Limite latência *peering* directo ultrapassado

Registos	Limite Ultrapassado	% Limite Ultrapassado
7017	17	0,21%

5.2.2 Teste latência PIX

A Figura 5.10 mostra a informação apresentada na página da interface Web para visualização do histórico de latência para este teste.

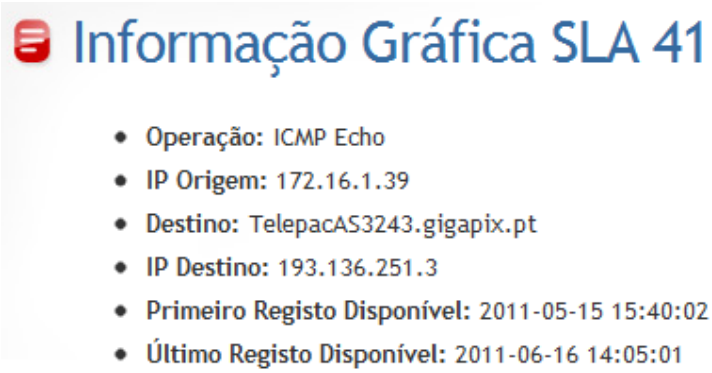


Figura 5.10 – Informação teste latência PIX

O histórico de latência de um dia, semana e mês é apresentado nas Figura 5.11, Figura 5.12 e Figura 5.13 respectivamente.

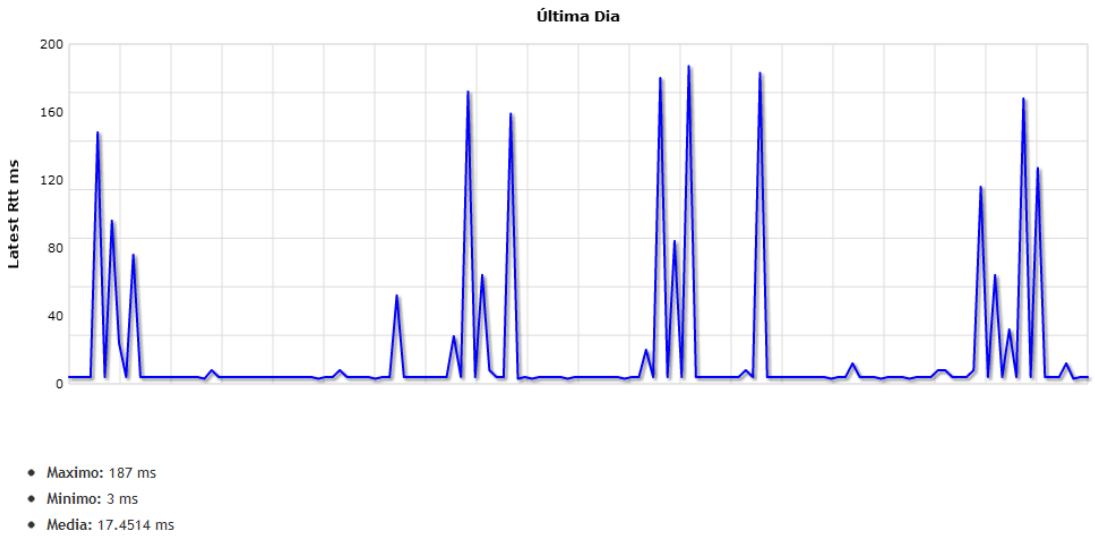


Figura 5.11 – Histórico latência PIX último dia

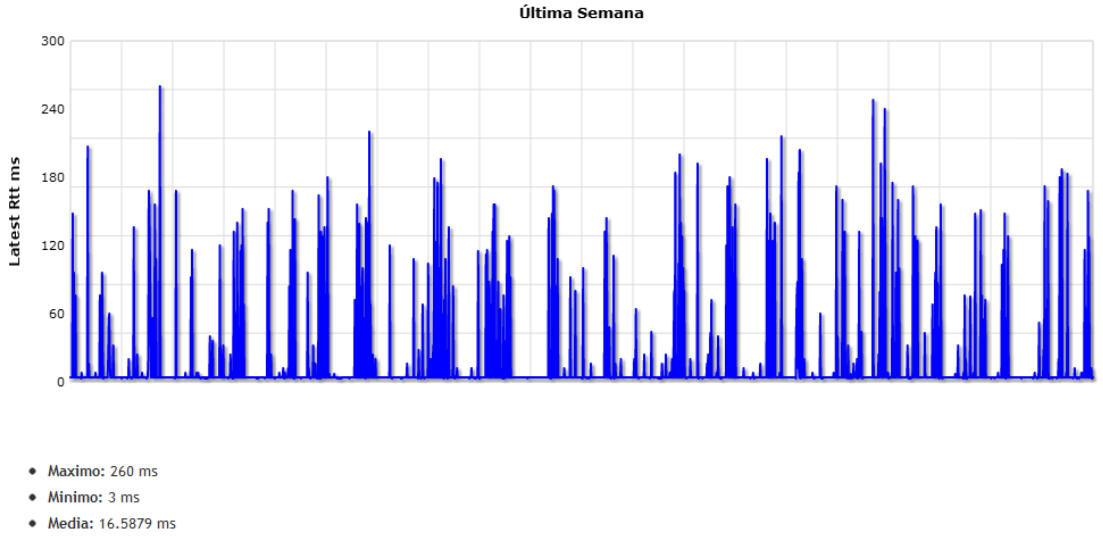


Figura 5.12 – Histórico latência PIX última semana

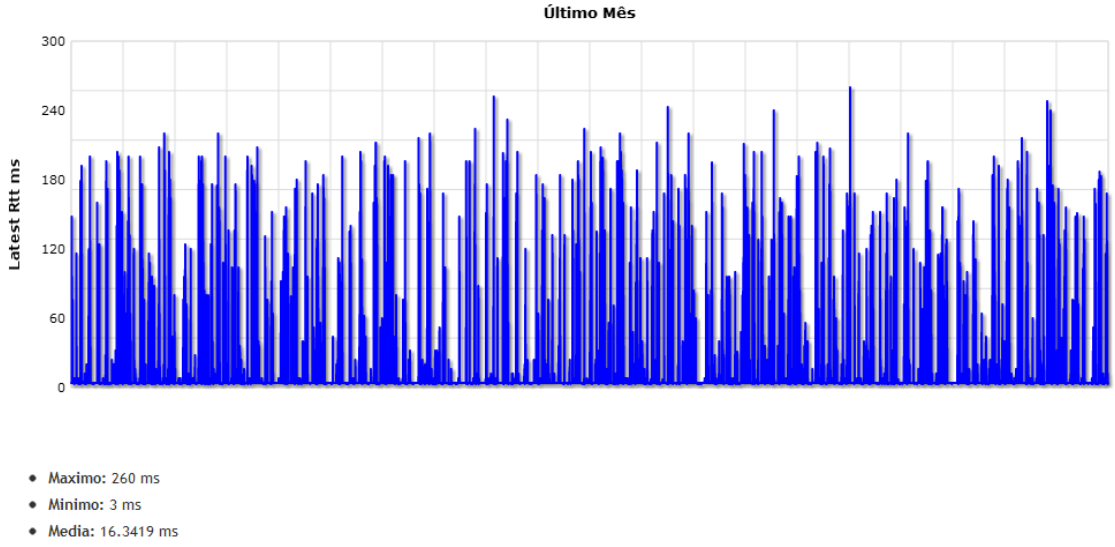


Figura 5.13 – Histórico latência PIX último mês

Na Tabela 5.9 são apresentados os valores de latência máxima, mínima e média.

Tabela 5.9 – Valores latência PIX

Período	Máximo (ms)	Mínimo (ms)	Média (ms)
15/05/2011 a 16/06/2011	260	3	16,3419
15/05/2011 a 02/06/2011	252	3	15,8839
02/06/2011 a 16/06/2011	260	3	17,0309

A Tabela 5.10 apresenta o número de vezes que o limite contratado para a métrica associada ao teste foi ultrapassado.

Tabela 5.10 – Limite latência PIX ultrapassado

Registos	Limite Ultrapassado	% Limite Ultrapassado
7023	824	11,73%

5.2.3 Teste latência tráfego Intraeuropeu

Na Figura 5.14 é apresentada a informação da página da interface Web para visualização do histórico de latência.

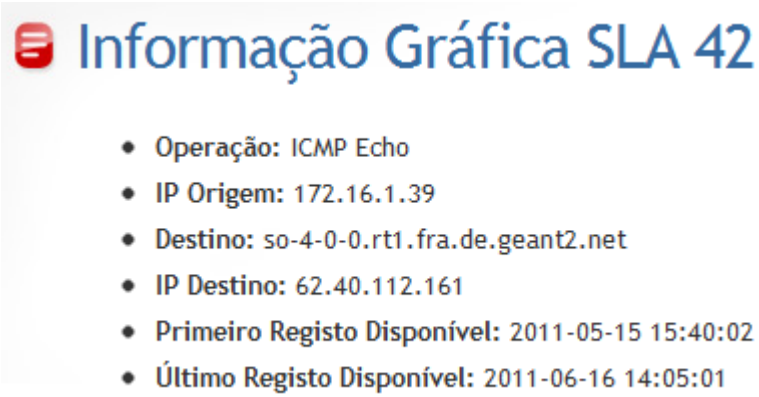


Figura 5.14 – Informação teste latência tráfego Intraeuropeu

O histórico de latência de um dia de teste é apresentado na Figura 5.15.

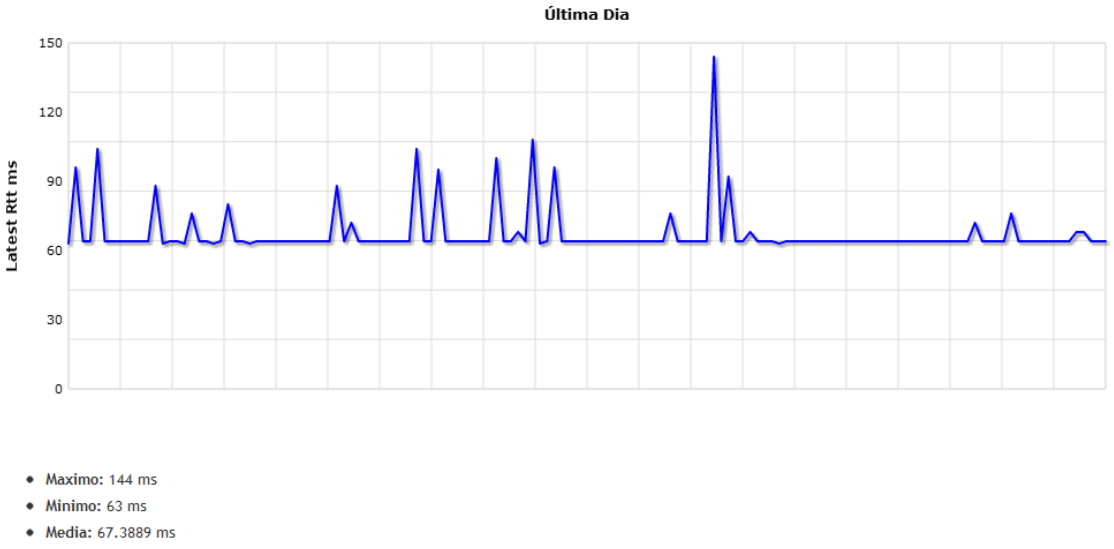


Figura 5.15 – Histórico latência tráfego Intraeuropeu último dia

Na Figura 5.16 é apresentado o histórico de latência de uma semana, enquanto na Figura 5.17 é apresentado o histórico de um mês.

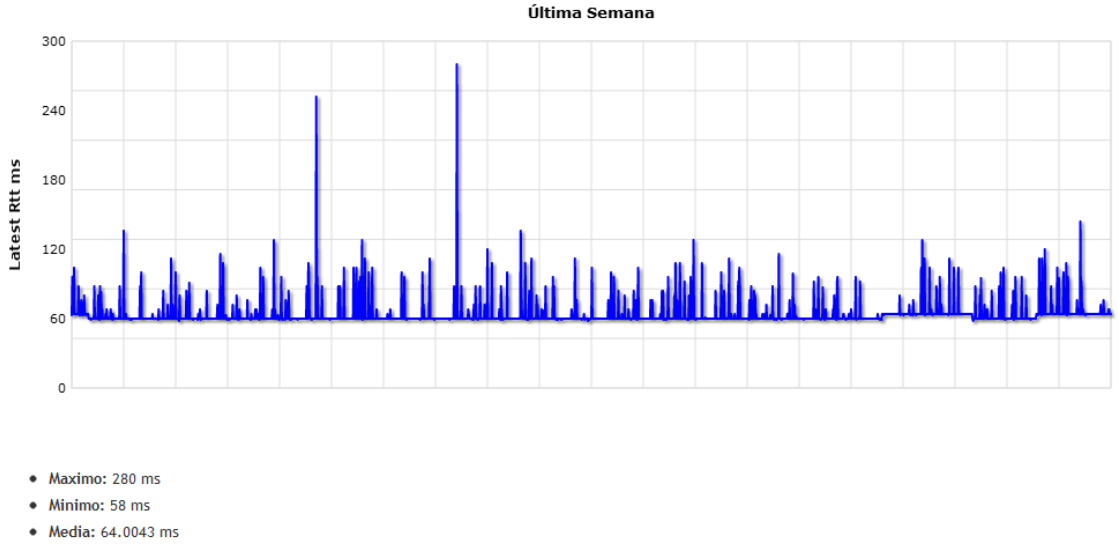


Figura 5.16 – Histórico latência tráfego Intraeuropeu última semana

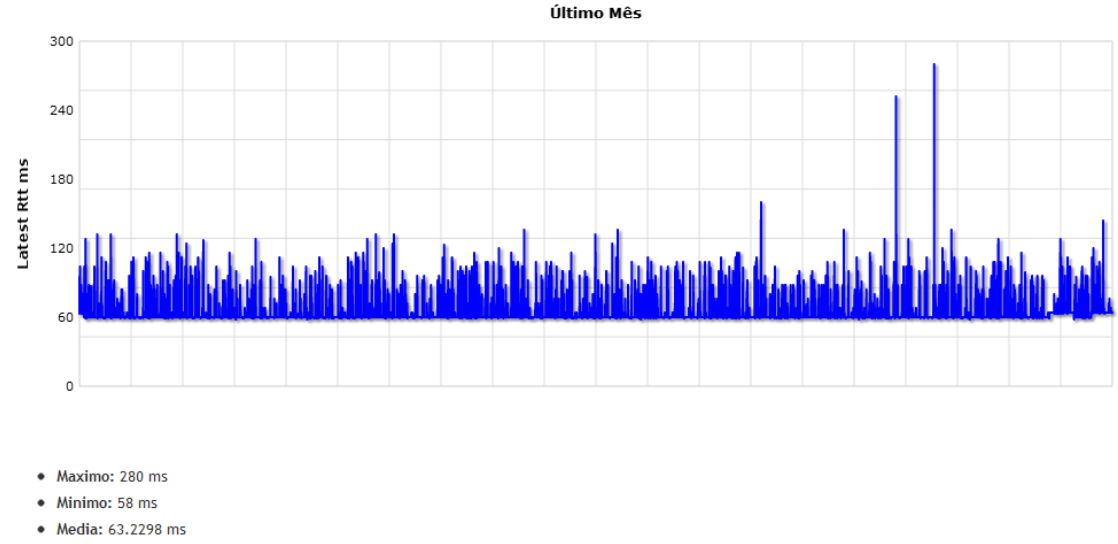


Figura 5.17 – Histórico latência tráfego Intraeuropeu último mês

Na Tabela 5.11 são apresentados os valores de latência máxima, mínima e média.

Tabela 5.11 – Valores latência tráfego Intraeuropeu

Período	Máximo (ms)	Mínimo (ms)	Média (ms)
15/05/2011 a 16/06/2011	280	58	63,2298
15/05/2011 a 02/06/2011	136	58	62,9429
02/06/2011 a 16/06/2011	280	58	63,7234

A Tabela 5.12 apresenta o número de vezes que o limite contratado para a métrica associada ao teste foi ultrapassado.

Tabela 5.12 – Limite latência tráfego Intraeuropeu ultrapassado

Registos	Limite Ultrapassado	% Limite Ultrapassado
7019	455	6,48%

5.2.4 Teste latência tráfego transatlântico

A Figura 5.18 mostra a informação apresentada na página da interface Web para visualização do histórico de latência para este teste.

Figura 5.18 – Informação teste latência tráfego Transatlântico

Para demonstrar o padrão de latência deste teste é apresentado o histórico de um dia na Figura 5.19.

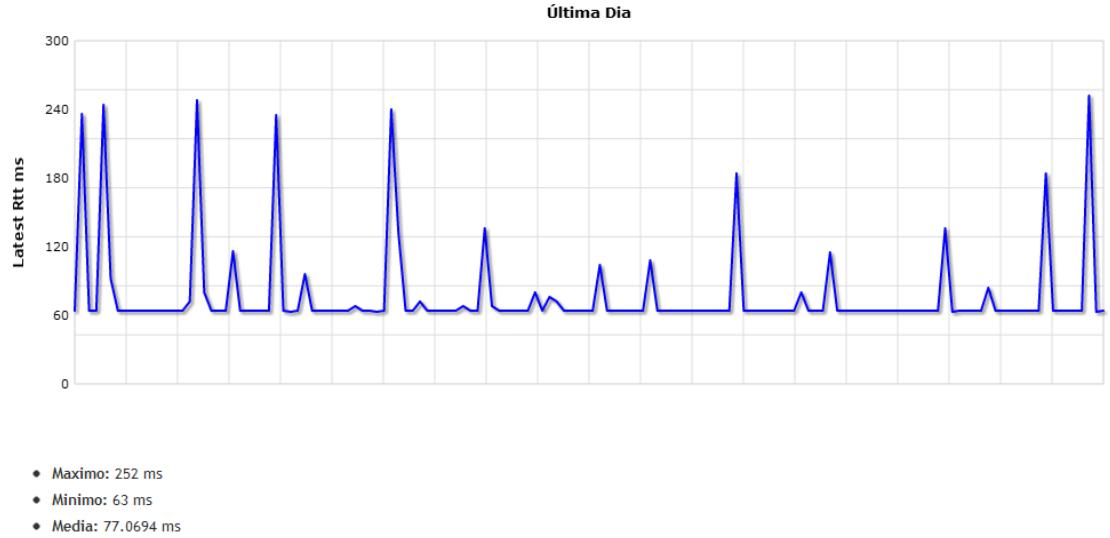


Figura 5.19 – Histórico latência tráfego Transatlântico último dia

O histórico de latência de uma semana é apresentado na Figura 5.20.

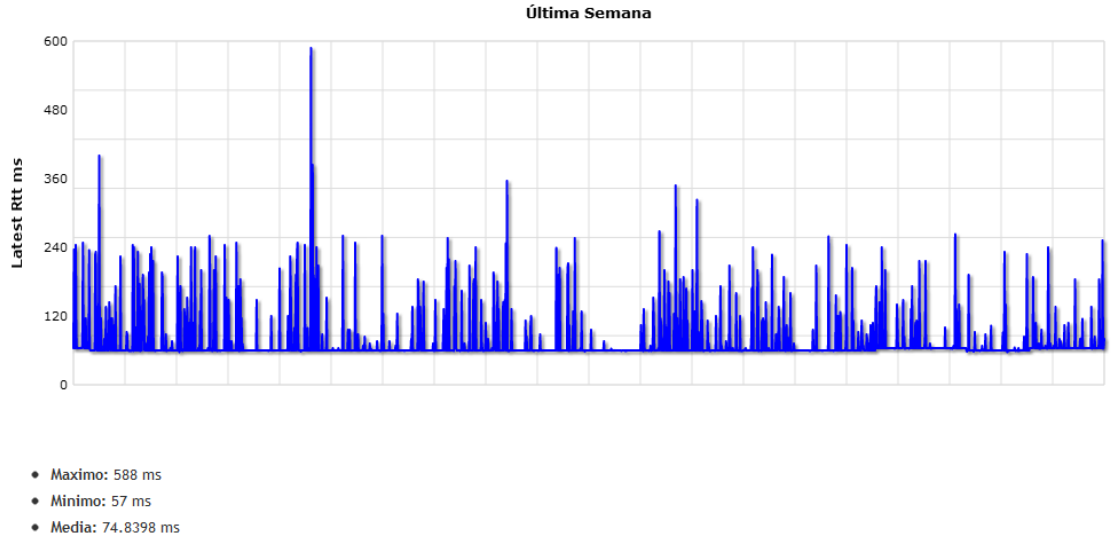


Figura 5.20 - Histórico latência tráfego Transatlântico última semana

O histórico de latência de um mês é apresentado na Figura 5.21.

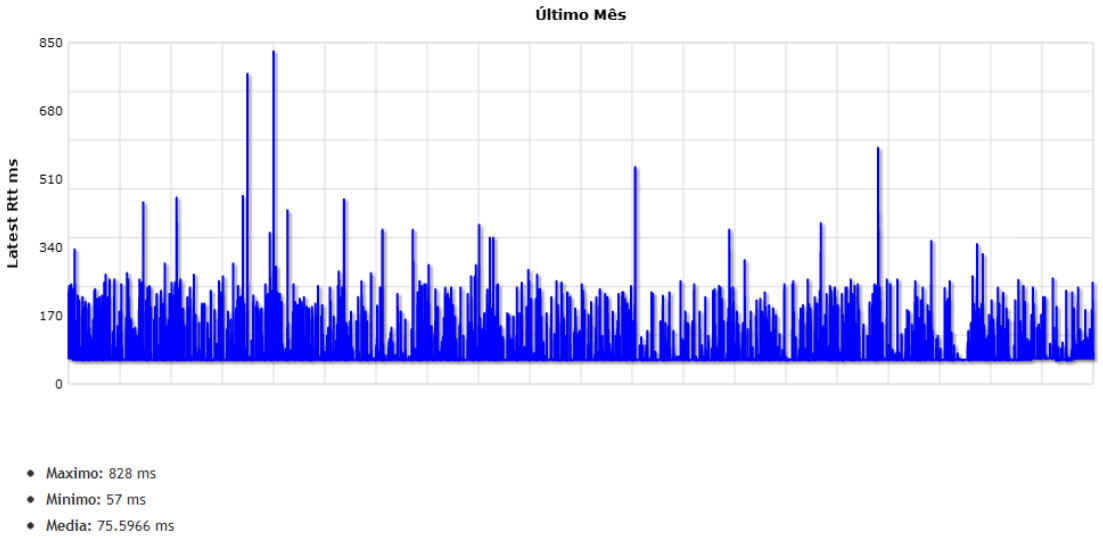


Figura 5.21 - Histórico latência tráfego Transatlântico último mês

Na Tabela 5.13 são apresentados os valores de latência máxima, mínima e média.

Tabela 5.13 - Valores latência tráfego Transatlântico

Período	Máximo (ms)	Mínimo (ms)	Média (ms)
15/05/2011 a 16/06/2011	828	57	75,5966
15/05/2011 a 02/06/2011	828	58	76,6732
02/06/2011 a 16/06/2011	588	57	74,0878

A Tabela 5.14 apresenta o número de vezes que o limite contratado para a métrica associada ao teste foi ultrapassado.

Tabela 5.14 - Limite latência tráfego Transatlântico ultrapassado

Registos	Limite Ultrapassado	% Limite Ultrapassado
7017	636	9,06%

5.2.5 Perda de pacotes

O período do teste efectuado, tal como no teste de latência foi entre 15/05/2011 e 16/06/2011. Os resultados alcançados são apresentados na Tabela 5.15.

Tabela 5.15: Resultados de teste perda de pacotes

IP	% Perda de Pacotes
193.137.0.10	0%
193.136.251.3	0%
62.40.112.161	0%
207.138.144.45	0%

Na interface Web é apresentada esta informação, tal como a Figura 5.22 mostra.

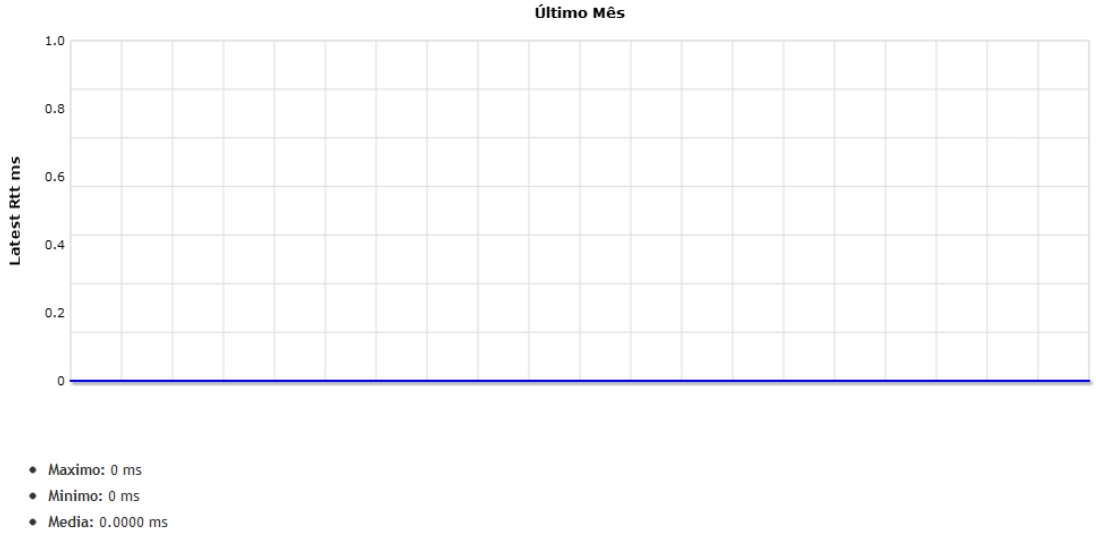


Figura 5.22 – Histórico Perda de Pacotes

5.2.6 Eventos, alertas e notificações

Os históricos de eventos, apresentado na Figura 5.23, alertas, apresentado na Figura 5.24, e notificações, apresentado na Figura 5.25, do sistema também foram mostrados na interface Web.

Eventos

Informação de Eventos

Data	Tipo	Descrição
2011-06-16 17:05:26	login	admin logged in the system
2011-06-16 17:05:10	database	Value for packet loss for 62.40.112.161 associated to contract id 1 inserted in database
2011-06-16 17:05:10	database	Value for packet loss for 207.138.144.45 associated to contract id 1 inserted in database
2011-06-16 17:05:10	database	Value for packet loss for 193.137.0.10 associated to contract id 1 inserted in database
2011-06-16 17:05:10	database	Value for packet loss for 193.136.251.3 associated to contract id 1 inserted in database
2011-06-16 17:05:01	database	Value for test sla 40 associated to contract id 1 inserted in database
2011-06-16 17:05:01	database	Value for test sla 42 associated to contract id 1 inserted in database
2011-06-16 17:05:01	database	Value for test sla 43 associated to contract id 1 inserted in database
2011-06-16 17:05:01	database	Value for test sla 41 associated to contract id 1 inserted in database
2011-06-16 17:00:10	database	Value for packet loss for 193.137.0.10 associated to contract id 1 inserted in database
2011-06-16 17:00:10	database	Value for packet loss for 193.136.251.3 associated to contract id 1 inserted in database
2011-06-16 17:00:10	database	Value for packet loss for 207.138.144.45 associated to contract id 1 inserted in database
2011-06-16 17:00:10	database	Value for packet loss for 62.40.112.161 associated to contract id 1 inserted in database
2011-06-16 17:00:01	database	Value for test sla 40 associated to contract id 1 inserted in database
2011-06-16 17:00:01	database	Value for test sla 43 associated to contract id 1 inserted in database
2011-06-16 17:00:01	database	Value for test sla 42 associated to contract id 1 inserted in database
2011-06-16 17:00:01	database	Value for test sla 41 associated to contract id 1 inserted in database

Figura 5.23 – Histórico Eventos

Alertas

Informação de Alertas

Data	Tipo	Estado	Descrição
2011-06-16 17:05:01	Latency Value	WARNING	Value for sla teste 41 in contract id 1 EXCEEDED the limit
2011-06-16 17:00:01	Latency Value	WARNING	Value for sla teste 43 in contract id 1 EXCEEDED the limit
2011-06-16 16:55:02	Latency Value	WARNING	Value for sla teste 42 in contract id 1 EXCEEDED the limit
2011-06-16 16:55:02	Latency Value	WARNING	Value for sla teste 43 in contract id 1 EXCEEDED the limit
2011-06-16 16:45:01	Latency Value	WARNING	Value for sla teste 43 in contract id 1 EXCEEDED the limit
2011-06-16 16:30:01	Latency Value	WARNING	Value for sla teste 43 in contract id 1 EXCEEDED the limit
2011-06-16 16:25:01	Latency Value	WARNING	Value for sla teste 41 in contract id 1 EXCEEDED the limit
2011-06-16 16:15:01	Latency Value	WARNING	Value for sla teste 42 in contract id 1 EXCEEDED the limit
2011-06-16 15:35:01	Latency Value	WARNING	Value for sla teste 42 in contract id 1 EXCEEDED the limit
2011-06-16 15:35:01	Latency Value	WARNING	Value for sla teste 40 in contract id 1 EXCEEDED the limit
2011-06-16 15:25:01	Latency Value	WARNING	Value for sla teste 41 in contract id 1 EXCEEDED the limit
2011-06-16 15:15:01	Latency Value	WARNING	Value for sla teste 43 in contract id 1 EXCEEDED the limit
2011-06-16 15:10:01	Latency Value	WARNING	Value for sla teste 43 in contract id 1 EXCEEDED the limit
2011-06-16 15:05:01	Latency Value	WARNING	Value for sla teste 43 in contract id 1 EXCEEDED the limit
2011-06-16 15:00:01	Latency Value	WARNING	Value for sla teste 43 in contract id 1 EXCEEDED the limit

Figura 5.24 – Histórico Alertas

Notificações

Informação de Notificações

Data	Tipo	Estado	Descrição
2011-06-16 17:10:02	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 42 EXCEEDED
2011-06-16 17:10:02	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 41 EXCEEDED
2011-06-16 17:05:01	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 41 EXCEEDED
2011-06-16 17:00:01	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 43 EXCEEDED
2011-06-16 16:55:02	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 42 EXCEEDED
2011-06-16 16:55:02	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 43 EXCEEDED
2011-06-16 16:52:14	ee02187@fe.up.pt	Status Report	Monthly Status Report send for sla test 42
2011-06-16 16:52:14	ee02187@fe.up.pt	Status Report	Monthly Status Report send for sla test 41
2011-06-16 16:52:14	ee02187@fe.up.pt	Status Report	Monthly Status Report send for sla test 43
2011-06-16 16:52:13	ee02187@fe.up.pt	Status Report	Monthly Status Report send for sla test 40
2011-06-16 16:45:01	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 43 EXCEEDED
2011-06-16 16:30:01	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 43 EXCEEDED
2011-06-16 16:25:01	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 41 EXCEEDED
2011-06-16 16:15:01	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 42 EXCEEDED
2011-06-16 15:40:01	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 40 EXCEEDED
2011-06-16 15:35:02	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 40 EXCEEDED
2011-06-16 15:35:02	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 42 EXCEEDED

Figura 5.25 – Histórico Notificações

Envio de emails

Como se pode verificar pelo histórico de notificações quando os limites dos testes eram ultrapassados eram enviados emails ao utilizador com essa informação. Na Figura 5.26, Figura 5.27, Figura 5.28 e Figura 5.29 é mostrado, para cada um dos testes, o envio deste tipo de emails para o utilizador.

De slaip@dissertacao.netlab.fe.up.pt
assunto **Limite contratado para SLA ultrapassado**
Para Meu FEUP

Informação SLA 40

Associado:

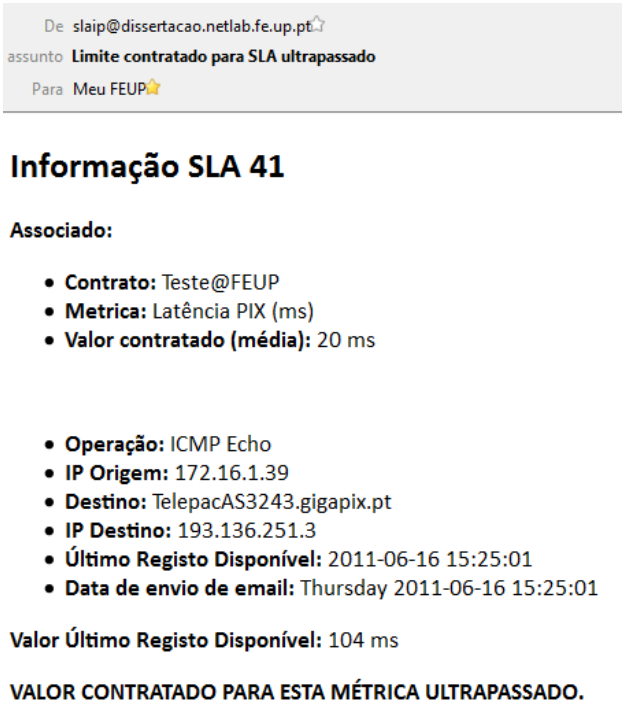
- **Contrato:** Teste@FEUP
- **Metrica:** Latência Peering Directo (ms)
- **Valor contratado (média):** 10 ms

- **Operação:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** Router3.10GE.Lisboa.fccn.pt
- **IP Destino:** 193.137.0.10
- **Último Registo Disponível:** 2011-06-16 15:35:01
- **Data de envio de email:** Thursday 2011-06-16 15:35:01

Valor Último Registo Disponível: 12 ms

VALOR CONTRATADO PARA ESTA MÉTRICA ULTRAPASSADO.

Figura 5.26: Email Limite latência *peering* directo ultrapassado



De slaip@dissertacao.netlab.fe.up.pt
assunto **Limite contratado para SLA ultrapassado**
Para Meu FEUP

Informação SLA 41

Associado:

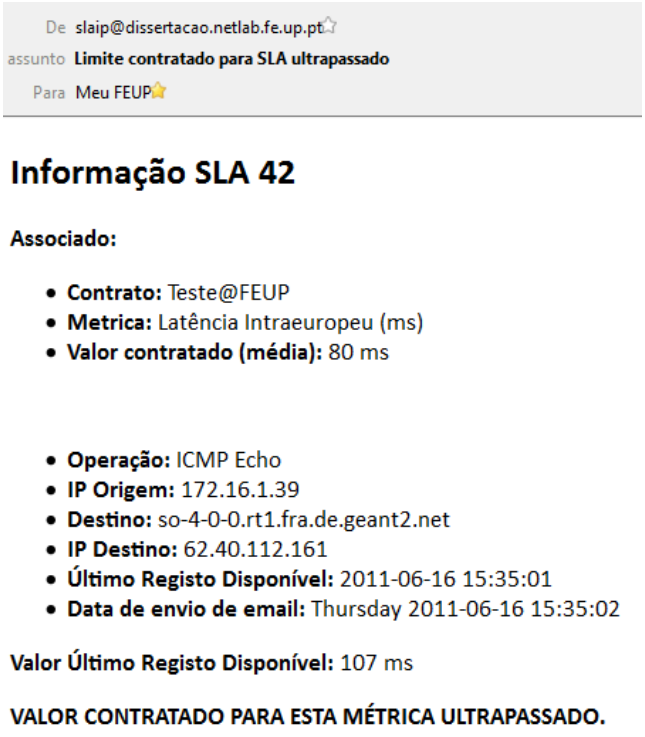
- **Contrato:** Teste@FEUP
- **Metrica:** Latência PIX (ms)
- **Valor contratado (média):** 20 ms

- **Operação:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** TelepacAS3243.gigapix.pt
- **IP Destino:** 193.136.251.3
- **Último Registo Disponível:** 2011-06-16 15:25:01
- **Data de envio de email:** Thursday 2011-06-16 15:25:01

Valor Último Registo Disponível: 104 ms

VALOR CONTRATADO PARA ESTA MÉTRICA ULTRAPASSADO.

Figura 5.27 - Email Limite latência PIX ultrapassado



De slaip@dissertacao.netlab.fe.up.pt
assunto **Limite contratado para SLA ultrapassado**
Para Meu FEUP

Informação SLA 42

Associado:

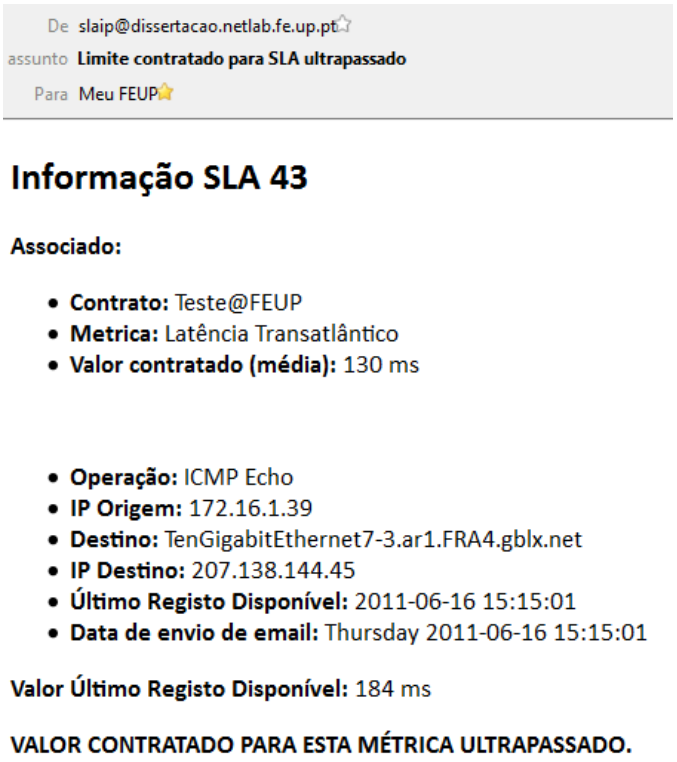
- **Contrato:** Teste@FEUP
- **Metrica:** Latência Intraeuropeu (ms)
- **Valor contratado (média):** 80 ms

- **Operação:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** so-4-0-0.rt1.fra.de.geant2.net
- **IP Destino:** 62.40.112.161
- **Último Registo Disponível:** 2011-06-16 15:35:01
- **Data de envio de email:** Thursday 2011-06-16 15:35:02

Valor Último Registo Disponível: 107 ms

VALOR CONTRATADO PARA ESTA MÉTRICA ULTRAPASSADO.

Figura 5.28 - Email Limite latência tráfego Intraeuropeu ultrapassado



De slaip@dissertacao.netlab.fe.up.pt
assunto **Limite contratado para SLA ultrapassado**
Para Meu FEUP

Informação SLA 43

Associado:

- **Contrato:** Teste@FEUP
- **Metrica:** Latência Transatlântico
- **Valor contratado (média):** 130 ms

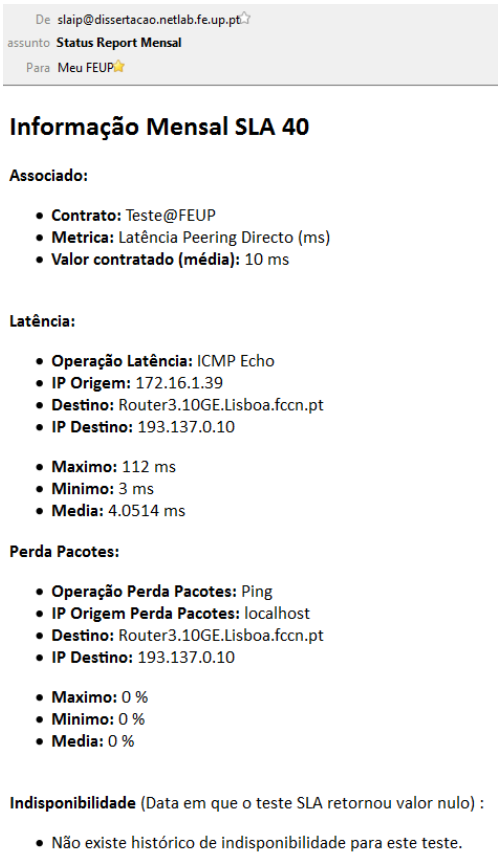
- **Operação:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** TenGigabitEthernet7-3.ar1.FRA4.gblx.net
- **IP Destino:** 207.138.144.45
- **Último Registo Disponível:** 2011-06-16 15:15:01
- **Data de envio de email:** Thursday 2011-06-16 15:15:01

Valor Último Registo Disponível: 184 ms

VALOR CONTRATADO PARA ESTA MÉTRICA ULTRAPASSADO.

Figura 5.29 - Email Limite latência tráfego Transatlântico ultrapassado

Também enviava, para cada um dos testes, relatórios com o histórico mensal de latência, perda de pacotes e períodos de indisponibilidade. Na Figura 5.30, Figura 5.31, Figura 5.32 e Figura 5.33 é mostrado, para cada um dos testes, o envio deste tipo de emails para o utilizador.



De slaip@dissertacao.netlab.fe.up.pt
assunto **Status Report Mensal**
Para Meu FEUP

Informação Mensal SLA 40

Associado:

- **Contrato:** Teste@FEUP
- **Metrica:** Latência Peering Directo (ms)
- **Valor contratado (média):** 10 ms

Latência:

- **Operação Latência:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** Router3.10GE.Lisboa.fccn.pt
- **IP Destino:** 193.137.0.10

- **Maximo:** 112 ms
- **Minimo:** 3 ms
- **Media:** 4.0514 ms

Perda Pacotes:

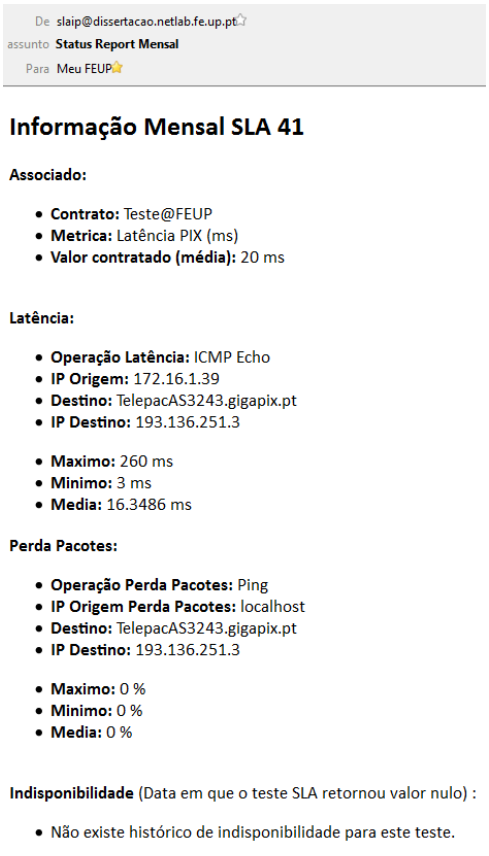
- **Operação Perda Pacotes:** Ping
- **IP Origem Perda Pacotes:** localhost
- **Destino:** Router3.10GE.Lisboa.fccn.pt
- **IP Destino:** 193.137.0.10

- **Maximo:** 0 %
- **Minimo:** 0 %
- **Media:** 0 %

Indisponibilidade (Data em que o teste SLA retornou valor nulo) :

- Não existe histórico de indisponibilidade para este teste.

Figura 5.30 - Email relatório mensal tráfego *peering* directo



De slaip@dissertacao.netlab.fe.up.pt
assunto **Status Report Mensal**
Para Meu FEUP

Informação Mensal SLA 41

Associado:

- **Contrato:** Teste@FEUP
- **Metrica:** Latência PIX (ms)
- **Valor contratado (média):** 20 ms

Latência:

- **Operação Latência:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** TelepacAS3243.gigapix.pt
- **IP Destino:** 193.136.251.3

- **Maximo:** 260 ms
- **Minimo:** 3 ms
- **Media:** 16.3486 ms

Perda Pacotes:

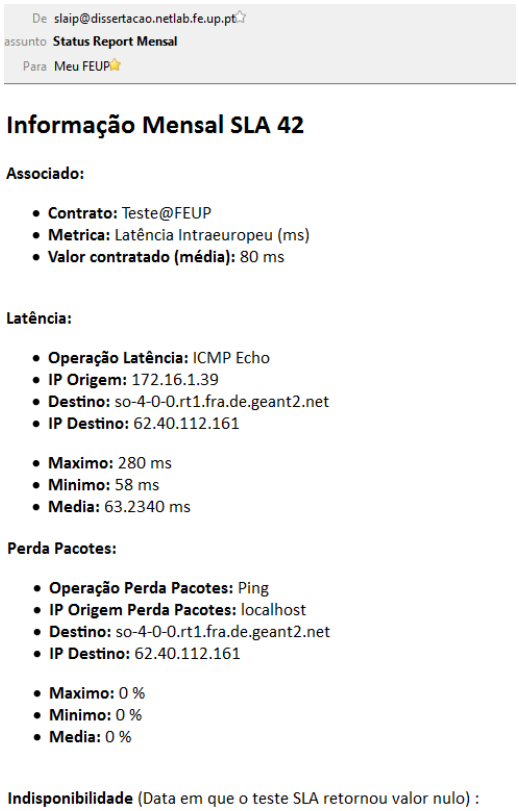
- **Operação Perda Pacotes:** Ping
- **IP Origem Perda Pacotes:** localhost
- **Destino:** TelepacAS3243.gigapix.pt
- **IP Destino:** 193.136.251.3

- **Maximo:** 0 %
- **Minimo:** 0 %
- **Media:** 0 %

Indisponibilidade (Data em que o teste SLA retornou valor nulo) :

- Não existe histórico de indisponibilidade para este teste.

Figura 5.31 - Email relatório mensal tráfego PIX directo



De slaip@dissertacao.netlab.fe.up.pt
assunto **Status Report Mensal**
Para Meu FEUP

Informação Mensal SLA 42

Associado:

- **Contrato:** Teste@FEUP
- **Metrica:** Latência Intraeuropeu (ms)
- **Valor contratado (média):** 80 ms

Latência:

- **Operação Latência:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** so-4-0-0.rt1.fra.de.geant2.net
- **IP Destino:** 62.40.112.161

- **Maximo:** 280 ms
- **Minimo:** 58 ms
- **Media:** 63.2340 ms

Perda Pacotes:

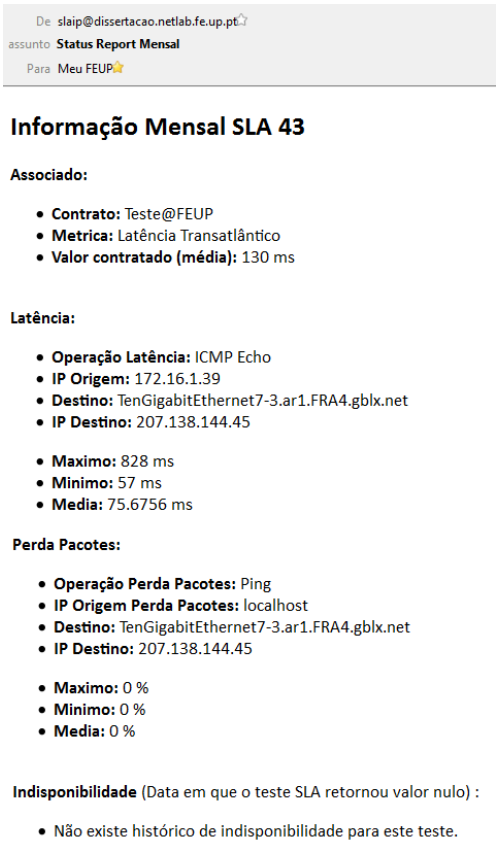
- **Operação Perda Pacotes:** Ping
- **IP Origem Perda Pacotes:** localhost
- **Destino:** so-4-0-0.rt1.fra.de.geant2.net
- **IP Destino:** 62.40.112.161

- **Maximo:** 0 %
- **Minimo:** 0 %
- **Media:** 0 %

Indisponibilidade (Data em que o teste SLA retornou valor nulo) :

- Não existe histórico de indisponibilidade para este teste.

Figura 5.32 - Email relatório mensal tráfego Intraeuropeu



De slaip@dissertacao.netlab.fe.up.pt
assunto **Status Report Mensal**
Para Meu FEUP

Informação Mensal SLA 43

Associado:

- **Contrato:** Teste@FEUP
- **Metrica:** Latência Transatlântico
- **Valor contratado (média):** 130 ms

Latência:

- **Operação Latência:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** TenGigabitEthernet7-3.ar1.FRA4.gblx.net
- **IP Destino:** 207.138.144.45

- **Maximo:** 828 ms
- **Minimo:** 57 ms
- **Media:** 75.6756 ms

Perda Pacotes:

- **Operação Perda Pacotes:** Ping
- **IP Origem Perda Pacotes:** localhost
- **Destino:** TenGigabitEthernet7-3.ar1.FRA4.gblx.net
- **IP Destino:** 207.138.144.45

- **Maximo:** 0 %
- **Minimo:** 0 %
- **Media:** 0 %

Indisponibilidade (Data em que o teste SLA retornou valor nulo) :

- Não existe histórico de indisponibilidade para este teste.

Figura 5.33 - Email relatório mensal tráfego Transatlântico

Para verificar o comportamento do sistema aquando da perda de conectividade com o equipamento, desligou-se momentaneamente o equipamento da rede. A Figura 5.34 mostra o histórico de alertas apresentado na interface com a indicação de perda de conectividade, a Figura 5.35 mostra o histórico de notificações apresentado na interface com a indicação de envio de *email* com essa informação. Já a Figura 5.36 mostra um desses *emails* enviados.

Informação de Alertas

Data	Tipo	Estado	Descrição
2011-06-17 14:10:07	Host Reachability	CRITICAL	Loss of connectivity to 172.16.1.39
2011-06-17 14:10:07	Host Reachability	CRITICAL	Loss of connectivity to 172.16.1.39
2011-06-17 14:10:07	Host Reachability	CRITICAL	Loss of connectivity to 172.16.1.39
2011-06-17 14:10:07	Host Reachability	CRITICAL	Loss of connectivity to 172.16.1.39

Figura 5.34 - Histórico de alertas de perda de conectividade com equipamento

Informação de Notificações

Data	Tipo	Estado	Descrição
2011-06-17 14:15:18	ee02187@fe.up.pt	Host Unreachable	Host for sla test 43 UNREACHABLE
2011-06-17 14:15:14	ee02187@fe.up.pt	Host Unreachable	Host for sla test 42 UNREACHABLE
2011-06-17 14:15:10	ee02187@fe.up.pt	Host Unreachable	Host for sla test 41 UNREACHABLE
2011-06-17 14:15:06	ee02187@fe.up.pt	Host Unreachable	Host for sla test 40 UNREACHABLE

Figura 5.35 - Histórico de notificações de perda de conectividade com equipamento

De slaip@dissertacao.netlab.fe.up.pt
assunto **Perda de Conectividade Equipamento**
Para Meu FEUP

Informação SLA 40

Associado:

- **Contrato:** Teste@FEUP
- **Metrica:** Latência Peering Directo (ms)
- **Valor contratado (média):** 10 ms

- **Operação:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** Router3.10GE.Lisboa.fccn.pt
- **IP Destino:** 193.137.0.10
- **Último Registo Disponível:** 2011-06-17 14:10:07
- **Data de envio de email:** Friday 2011-06-17 14:15:06

Valor último registo obtido da base de dados nulo.

Informação fping ao equipamento: 172.16.1.39 is unreachable

PERDA DE CONECTIVIDADE COM O EQUIPAMENTO.

Figura 5.36 - *Email* perda de conectividade com equipamento

Para simular o comportamento do sistema aquando da perda de conectividade do equipamento com o IP de destino, ligou-se novamente o equipamento à rede. Desta forma, para alguns dos testes, foi possível o script de recolha de dados ir recuperar o último valor do equipamento que era nulo e dessa forma proceder ao envio de alertas para o sistema e notificações para o utilizador. A Figura 5.37 mostra o histórico de alertas, a Figura 5.38 o histórico de notificações enviadas e a Figura 5.39 mostra um dos *emails* enviados para o utilizador.

Informação de Alertas

Data	Tipo	Estado	Descrição
2011-06-17 14:35:01	Latency Value	WARNING	Value for sla teste 41 in contract id 1 EXCEEDED the limit
2011-06-17 14:20:01	Latency Value	CRITICAL	Value for sla teste 40 in contract id 1 is NULL
2011-06-17 14:20:01	Latency Value	CRITICAL	Loss of connectivity to destiny 193.136.251.3
2011-06-17 14:20:01	Latency Value	CRITICAL	Value for sla teste 42 in contract id 1 is NULL
2011-06-17 14:20:01	Latency Value	CRITICAL	Loss of connectivity to destiny 62.40.112.161

Figura 5.37 – Histórico de alertas perda conectividade com o destino

Informação de Notificações

Data	Tipo	Estado	Descrição
2011-06-17 14:35:01	ee02187@fe.up.pt	Test Limit Exceeded	Limit value for sla test 41 EXCEEDED
2011-06-17 14:20:02	ee02187@fe.up.pt	Destiny Unreachable	Destiny IP for sla test 41 UNREACHABLE
2011-06-17 14:20:02	ee02187@fe.up.pt	Destiny Unreachable	Destiny IP for sla test 42 UNREACHABLE

Figura 5.38 – Histórico de notificações perda conectividade com o destino

De slaip@dissertacao.netlab.fe.up.pt
assunto **Perda de Conectividade IP Destino SLA**
Para Meu FEUP

Informação SLA 41

Associado:

- **Contrato:** Teste@FEUP
- **Metrica:** Latência PIX (ms)
- **Valor contratado (média):** 20 ms

- **Operação:** ICMP Echo
- **IP Origem:** 172.16.1.39
- **Destino:** TelepacAS3243.gigapix.pt
- **IP Destino:** 193.136.251.3
- **Último Registo Disponível:** 2011-06-17 14:20:01
- **Data de envio de email:** Friday 2011-06-17 14:20:02

Valor último registo obtido da base de dados nulo.

Informação fping ao equipamento: 172.16.1.39 is alive

PERDA DE CONECTIVIDADE COM O IP DE DESTINO.

Figura 5.39 – *Email* perda conectividade com o destino

5.3 Discussão de Resultados

Deve-se chamar atenção ao facto dos testes terem sido efectuados num laboratório em que decorriam aulas e como tal houve períodos em que o equipamento de teste teve de ser reconfigurado para permitir aos alunos a realização dos seus trabalhos. Assim se explica que para um período de teste de 33 dias, que deveria resultar em cerca de 9200 registos, só se tenham alcançado pouco mais de 7000 para cada um dos testes.

Apesar disto, o número obtido já permitiu uma boa base de análise do funcionamento do sistema. Foi criada a Tabela 5.16 com algumas das estatísticas recolhidas nos testes efectuados.

Tabela 5.16 – Estatísticas recolhidas nos testes

IP Teste	Média (ms)	Limite Ultrapassado	Perda Pacotes	Disponibilidade
193.137.0.10	4,0511	0,21%	0%	100%
193.137.251.3	16,3419	11,73%	0%	100%
62.40.112.161	63,2298	6,48%	0%	100%
207.138.144.45	75,5966	9,06%	0%	100%

Pode-se verificar, tendo em conta o cenário de teste apresentado, que não existiu perda de pacotes para nenhum dos IPs de teste, que o nível de disponibilidade de rede foi completo e as médias de latência ficaram todas abaixo dos limites propostos para cada uma delas, ou seja que os limites propostos não foram ultrapassados para nenhuma das métricas.

Verificou-se que ao nível de registos em que o limite teórico do cenário de teste foi ultrapassado o comportamento seguido foi o esperado. Para tráfego de *peering* directo a percentagem de vezes foi muito menor em relação ao tráfego Transatlântico. No entanto verificou-se que no caso do teste para tráfego para o PIX essa percentagem foi a mais acentuada e que no padrão de latência se pôde observar picos elevados chegando a atingir um valor máximo de 260 milissegundos. Isto pode ser explicado pelo router utilizado para o teste ser da Telepac e os seus routers serem os que apresentam maior carga de tráfego ao nível nacional, provocando dessa forma um aumento dos valores de latência em algumas ocasiões. Em relação aos eventos, alertas e notificações gerados pelo sistema, verificou-se que estes respondem de acordo com as situações criadas, dando informação importante ao utilizador quer ao nível da interface Web quer ao nível de notificações sobre o estado dos testes.

Capítulo 6

Conclusões

Este último capítulo apresenta uma síntese do trabalho apresentado no documento, referindo os resultados obtidos e as conclusões alcançadas. São também apresentadas as perspectivas de desenvolvimento futuro.

6.1 Síntese do trabalho desenvolvido

O trabalho desenvolvido levou à criação de uma ferramenta de monitorização e gestão de SLA IP através da recolha de dados associados e posterior visualização dos mesmos, aproveitando a tecnologia IP SLA já existente nos equipamentos Cisco presentes no laboratório de redes da FEUP.

A fase inicial do trabalho centrou-se no estudo de SLA e SLA IP de forma a tentar perceber as suas potencialidades, limitações, e quais os níveis serviços e principais métricas usadas neste tipo de contratos.

De seguida foi efectuada um estudo e análise da tecnologia Cisco IOS IP SLA e de diferentes ferramentas de monitorização e gestão de SLA, comerciais e *open source*, disponíveis no mercado.

Passou-se então para o desenvolvimento do sistema, onde se desenvolveu uma ferramenta a partir de aplicações e linguagens de programação livres da qual era possível não só a monitorização de valores de métricas, mas também a configuração automática de operações IP SLA nos equipamentos, visualização de alertas e eventos do sistema, associação de testes a métricas e contratos e envio de notificações ao utilizador aumentando as funcionalidades habituais em ferramentas *open source* para este tipo de situação.

Por último concretizou-se a validação da solução através dos testes efectuados, podendo-se afirmar que os objectivos principais desta dissertação foram cumpridos.

6.2 Desenvolvimento Futuro

Apesar de a solução apresentada permitir a monitorização e gestão de contratos, ela pode ser enriquecida pela inclusão das seguintes funcionalidades:

- Melhoria da interface Web com a inclusão de novos elementos como por exemplo utilização da função *date picker* para permitir a visualização de dados para períodos especificados pelo utilizador, possibilidade de ampliação de imagem dos gráficos, criação de relatórios de valores e gráficos para ficheiros *Portable Document Format* (PDF) ou *MS Excel file extension* (XLS) e criação de cópia de segurança da base de dados;
- Permitir a identificação automática de equipamentos com suporte à tecnologia Cisco IOS IP SLA;
- Permitir a configuração da totalidade das operações IP SLA suportadas por esta tecnologia;
- Expandir o número de métricas a apresentar;
- Permitir o envio de notificações ao utilizador por SMS;
- Permitir o envio de logs para um servidor remoto.

Referências

1. **Neves, João.** Planeamento: Análise de Requisitos. [Online] [Citação: 25 de Maio de 2011.] http://www.inescporto.pt/~jneves/feup/2010-2011/pgre2s/requirements.pdf.

2. *Service Level Agreements on IP Networks.* **Verma, Dinesh C.** 9, s.l. : Proceedings of the IEEE, 2004, Vol. 92, pp. 1382-1388. ISSN: 0018-9219.

3. **Bouman, Jacques, Trienekens, Jos e van der Zwan, Mark.** *Specification Of Service Level Agreements, Clarifying On The Basis Of Practical Research.* Washington DC : IEEE Computer Society, 1999. ISBN: 0-7695-0328-4.

4. Cisco IOS IP Service Level Agreements Q&A. [Online] [Citação: 16 de Junho de 2011.] http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_qas0900aecd8017bd5a.html.

5. *Cisco Ip SLA Overview 15.1mt.* [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1mt/Cisco_IOS_IP_SLAs_Overview.html.

6. [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/i/100001-200000/120001-130000/121001-122000/121381.jpg.

7. Cisco IOS IP Service Level Agreements User Guide. [Online] [Citação: 16 de Junho de 2011.] http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.html.

8. [Online] [Citação: 16 de Junho de 2011.] http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/images/technologies_white_paper09186a00802d5efe-01.jpg.

9. *Cisco IOS IP SLA ICMP-Echo Operation*. [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1mt/Configuring_Cisco_IOS_IP_SLAs_ICMP_Echo_Operations.html.

10. [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/i/100001-200000/120001-130000/121001-122000/121419.jpg.

11. *Cisco IOS IP SLA HTTP Operation*. [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1mt/Configuring_Cisco_IOS_IP_SLAs_HTTP_Operations.html.

12. *Cisco IOS IP SLA DNS Operation*. [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1mt/Configuring_Cisco_IOS_IP_SLAs_DNS_Operations.html.

13. [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/i/000001-100000/15001-20000/18001-18500/18171.jpg.

14. *Cisco IOS IP SLA DHCP Operation*. [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1mt/Configuring_Cisco_IOS_IP_SLAs_DHCP_Operations.html.

15. *Cisco IOS IP SLA FTP Operation*. [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1mt/Configuring_Cisco_IOS_IP_SLAs_FTP_Operations.html.

16. [Online] [Citação: 10 de Junho de 2011.] http://www.cisco.com/en/US/i/000001-100000/35001-40000/38001-38500/38175.jpg.

17. *Solarwinds*. [Online] [Citação: 11 de Junho de 2011.] http://www.solarwinds.com/.

18. *Orion NPM*. [Online] [Citação: 11 de Junho de 2011.] http://www.solarwinds.com/products/orion/.

19. *Orion IP SLA Manager*. [Online] [Citação: 11 de Junho de 2011.] http://www.solarwinds.com/products/orion/ip_sla_monitoring/.

20. *Dorado Software*. [Online] [Citação: 16 de Junho de 2011.] http://www.doradosoftware.com.

21. *Redcell Advanced Monitor - Cisco IP SLA*. [Online] [Citação: 16 de Junho de 2011.] http://www.doradosoftware.com/solutions/cisco-ipsla-solutions.html.

22. *Nimsoft Monitor*. [Online] [Citação: 15 de Junho de 2011.] http://www.nimsoft.com/solutions/nimsoft-monitor/network/cisco-ip-sla.

23. *Entuity*. [Online] [Citação: 15 de Junho de 2011.] http://www.entuity.com/products/index.html.

24. *EYE IP SLA Module*. [Online] [Citação: 15 de Junho de 2011.] http://www.entuity.com/collateral/ds/EYE-IPSLA-Module-Datasheet.pdf.

25. *Nagios Página Oficial*. [Online] [Citação: 08 de Junho de 2011.] http://www.nagios.org/.

26. **Barth, Wolfgang.** *Nagios: System and Network Monitoring*. 1st. 2006. pp. 16-18. ISBN 1-59327-070-4.

27. **Contributors, Nagios Core Development Team and Community.** Nagios Core Version 3.x Documentation. [Online] [Citação: 26 de Junho de 2010.] http://nagios.sourceforge.net/docs/nagios-3.pdf.

28. [Online] [Citação: 23 de Maio de 2011.] http://exchange.nagios.org/.

29. [Online] [Citação: 23 de Maio de 2011.] http://www.nagios.org/download/plugins.

30. *Nagios Plugin SLA*. [Online] [Citação: 06 de Junho de 2011.] http://exchange.nagios.org/directory/Plugins/Network-Connections,-Stats-and-Bandwidth/check_cisco_ipsla/details.

31. *Cacti Site Oficial*. [Online] [Citação: 05 de Junho de 2011.] http://www.cacti.net/.

32. **Kundu, Dinangkur e Lavlu, S. M. Ibrahim.** *Cacti 0.8 Network Monitoring*. s.l. : Packt Publishing, 2009. ISBN 978-1-847195-96-8.

33. *Cacti Template SLA*. [Online] [Citação: 05 de Junho de 2011.] http://forums.cacti.net/about19542.html.

34. *Zenoss Sítio Oficial*. [Online] [Citação: 03 de Junho de 2011.] http://www.zenoss.com/.

35. Zenoss Administration 3.0. [Online] [Citação: 04 de Junho de 2011.] http://community.zenoss.org/community/documentation/official_documentation/zenoss-guide/3.0-v03.

36. *Community: ZenPacks*. [Online] [Citação: 04 de Junho de 2011.] http://community.zenoss.org/community/zenpacks.

37. *Cisco IP SLA ZenPack*. [Online] [Citação: 04 de Junho de 2011.] http://community.zenoss.org/docs/DOC-3402.

38. Open NMS. [Online] [Citação: 10 de Junho de 2011.] http://www.opennms.org/.

39. *Main Page - Open NMS*. [Online] [Citação: 10 de Junho de 2011.] http://www.opennms.org/wiki/Main_Page.

40. *Cisco IP SLA Monitor - Open NMS*. [Online] [Citação: 10 de Junho de 2011.] http://www.opennms.org/wiki/Cisco_IP_SLA_Monitor.

41. *Cisco IP SLA Support - Open NMS*. [Online] [Citação: 10 de Junho de 2011.] http://www.opennms.org/wiki/Cisco_IP_SLA_Support.

42. *PHP*. [Online] [Citação: 10 de Março de 2011.] http://www.php.net/.

43. *jQuery*. [Online] [Citação: 22 de Abril de 2011.] http://jquery.com/.

44. *jQueryUI*. [Online] [Citação: 29 de Abril de 2011.] http://jqueryui.com/.

45. *JavaScript*. [Online] [Citação: 18 de Junho de 2011.] https://developer.mozilla.org/en/JavaScript.

46. *MySQL*. [Online] [Citação: 18 de Junho de 2011.] http://www.mysql.com/.

47. *RGraph*. [Online] [Citação: 28 de Março de 2011.] http://www.rgraph.net/.

48. *PHP-Telnet*. [Online] [Citação: 28 de Abril de 2011.] http://www.geckotribe.com/php-telnet/.

49. *Debian Lenny*. [Online] [Citação: 18 de Junho de 2011.] http://wiki.debian.org/DebianLenny.

50. *Apache*. [Online] [Citação: 10 de Março de 2011.] http://httpd.apache.org/.

51. [Online] [Citação: 05 de Maio de 2011.] http://www.computing.net/answers/linux/telnet-and-rsh-problem/29530.html.

52. *PHPMyadmin*. [Online] [Citação: 10 de Março de 2011.] http://www.phpmyadmin.net/.