INSTITUTO SUPERIOR DE TRANSPORTES E COMUNICAÇÕES

PROJECTO E IMPLEMENTAÇÃO DE UM SISTEMA DE MONITORIZAÇÃO DE REDE NO ISUTC

Micas Camela Manuel Rafael

Projecto Final do Curso

Curso de Licenciatura em Engenharia Informática e de Telecomunicações

Eng.º Elton Pedro Sixpence

Departamento de Tecnologias de Informação e Comunicação

Novembro de 2010

INSTITUTO SUPERIOR DE TRANSPORTES E COMUNICAÇÕES

PROJECTO E IMPLEMENTAÇÃO DE UM SISTEMA DE MONITORIZAÇÃO DE REDE NO ISUTC

Micas Camela Manuel Rafael

Projecto Final do Curso

Curso de Licenciatura em Engenharia Informática e de Telecomunicações

Eng.º Elton Pedro Sixpence

Departamento de Tecnologias de Informação e Comunicação

Novembro de 2010

Projecto e Implementação de um Sistema de Monitorização de Rede no ISUTC
Micas Camela Manuel Rafael

ÍNDICE

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado saúde e inteligência para concluir este trabalho.

Aos meus pais, Manuel Camela e Isaura Cuambe, por tudo que me ensinaram e por sempre terem me mostrado a importância da educação.

Ao meu tio Jaime Cuambe pela ajuda que sempre se dispôs a dar.

Ao meu primo Humberto Uamusse pelo aconselhamento prestado.

A toda minha família pelo apoio que me deram neste período, compreendendo a importância desta etapa da minha vida.

Ao Eng.º Elton Pedro Sixpence pelo seu trabalho de orientação, sem o qual a elaboração deste trabalho não seria possível.

Ao professor Mário Malagón pela ajuda na escolha do tema.

A Márcia por todo o carinho, apoio e atenção que sempre demonstrou em todas as etapas desta caminhada, principalmente nos momentos difíceis.

Aos meus amigos Danilo Bhangy, Agnalda da Graça, Sheyla Cassy, Dalila Annette, Carmen Rodrigues, Teresa Isabel, José Domingos, Raimundo Manuel, Timóteo Júnior, Filipe Chissequere, Frederick Suluda, Aissa Faquir, que me ajudaram sempre que possível.

Ao meu grupo Bengala pela força que sempre me foi dada.

Aos meus colegas de turma, que tornaram todos os 5 anos de formação mais fáceis.

A todos os professores que contribuíram para esta longa caminhada.

DEDICATÓRIA

"Aos meus pais Manuel e Isaura,
minha irmã Márcia,
meus primos Euclídio, Maria Lina e Lúcia
pelo apoio incondicional
em todos os momentos"

DECLARAÇÃO DE HONRA

Eu, Micas Camela Manuel Rafael declaro por minha honra que o presente Projecto Final do Curso é exclusivamente de minha autoria, não constituindo cópia de nenhum trabalho realizado anteriormente e as fontes usadas para a realização do trabalho encontram-se referidas na bibliografia.

Assinatura: _____

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

LISTA DAS ABREVIATURAS UTILIZADAS

AP	*Access Point*
CGI	*Common Gateway Interface*
CMIP	*Common Management Information Protocol*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
FIFO	*First In First Out*
FTP	*File Transfer Protocol*
HDD	*Hard Disk Drive*
HTTP	*Hypertext Transfer Protocol*
IAB	*Internet Architecture Board*
IETF	*Internet Engineering Task Force*
IMAP	*Internet Message Access Protocol*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
ITU	*International Telecommunication Union*
LAN	*Local Area Network*
LDAP	*Lightweight Directory Access Protocol*
LTS	*Long Term Support*
MIB	*Management Information Base*
MT	Meticais
NMA	*Network Management Agent*
NOC	*Network Operation Center*
NRPE	*Nagios Remote Plugin Executor*
OSI	*Open Systems Interconnection*
PHP	*PHP: Hypertext Processor*
POP	*Post Office Protocol*
RAM	*Random Access Memory*
RFC	*Request For Comment*
SLA	*Service Level Availability*
SMI	*Structure of Management Information*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*

SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TCP	*Transfer Control Protocol*
TIC	Tecnologia de Informação e Comunicação
TMN	*Telecomunication Management Network*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

RESUMO

As redes de computadores vem sendo o elemento principal para o funcionamento das organizações a nível mundial, esse facto surge da quantidade de benefícios que as redes proporcionam. Em contrapartida surge a necessidade de garantir o pleno funcionamento delas, pois se não for tomada a devida atenção, com a falha da rede, o funcionamento da empresa ficará comprometido. O ISUTC tem também como um dos seus elementos principais a sua rede de computadores, e com a integração de vários serviços de rede e pela rápida expansão da rede do ISUTC, tornou-se imprescindível o uso de um sistema de gestão de rede que pudesse auxiliar os administradores de rede do ISUTC, de modo a poder fornecer informações em tempo real sobre o estado de operação dos elementos de rede. De modo a responder as necessidades descritas, concluiu-se que seria de grande importância, a implementação de um sistema de gestão de rede. Como resposta ao problema, foi elaborado um estudo sobre sistemas de gestão de rede, concentrando-se mais nos de monitorização. Existindo vários modelos de gestão, foram seleccionados os sistemas de monitorização que mais se adequaram aos modelos que se pretendiam usar. De seguida os sistemas foram avaliados e foi escolhido o que melhor avaliação apresentou.

No final foram analisados os resultados que o sistema apresentou, sendo o resultado principal uma descrição detalhada da operação dos servidores e serviços de rede.

PALAVRAS CHAVE: rede; monitorização; implementação.

CAPÍTULO 1 INTRODUÇÃO

1.1 Introdução

Na presente era das TICs (Tecnologias de Informação e Comunicação), as empresas buscam no mundo da informática soluções que de um modo geral, possibilitem a colecta, o transporte, o processamento e a disseminação das informações com as quais as empresas lidam e tomam conta. Deste modo a solução mais empregue tem sido, o uso de computadores que são utilizados para criar, modificar e guardar as informações das empresas.

Segundo Tanembaum (2003, p. 3), “Toda empresa de grande e médio porte e muitas empresas pequenas têm uma dependência vital de informações computadorizadas.”.

De forma a tornar essa solução mais eficaz, as TICs têm sido implementadas com suporte em redes de computadores, que possibilitam atingir os propósitos de sua implementação.
Utilizando as redes de computadores como suporte, os computadores que visam tratar das informações das empresas passam a estar interconectados. Sendo aqui, a questão da partilha de informação e recursos, o mais importante, o objectivo é tornar todos os programas, equipamentos e especialmente dados ao alcance de todas as pessoas na rede, independentemente da localização física do recurso e do utilizador.

Actualmente, as redes de computadores existentes nas empresas, instituições e ou organizações, têm sido projectadas de modo a prever a sua expansão no que diz respeito a capacidade de utilizadores que poderão partilhar os recursos e serviços existentes na rede. O uso de recursos e serviços existentes em tais redes tem o intuito de facilitar o trabalho dos funcionários e utilizadores gerais na partilha e troca de informações de modo flexível acelerando a execução das suas tarefas e deveres, na comunicação imediata sem abandonar os seus postos de trabalho, e no uso de periféricos de rede como por exemplo impressoras por vários utilizadores.

Após a implementação da rede, serviços de redes são implementados, que visam habilitar o uso dos recursos existentes e a disponibilização de informações na rede.

Normalmente, durante a operação da rede, os serviços nela implementados têm sido alvos de avarias, que são devidos a erros de *software* e ou de *hardware* comprometendo o

funcionamento da empresa, pois os utilizadores que mais utilizam esses serviços ficam impossibilitados de realizar as suas funções.

O problema com o qual as empresas se deparam no uso de redes de computadores, é o tempo de detecção, e resposta na resolução das avarias que ocorrem. Sendo que para uma empresa que tem informações vitais circulando pela rede, é de carácter importante que o problema seja identificado no menor tempo possível de modo a restabelecer o funcionamento normal da rede.

Para a detecção de avarias em nos periféricos e serviços implementados em redes de computadores, usam-se os denominados Sistema de Monitorização de Rede que têm como objectivo fazer o acompanhamento contínuo dos serviços e periféricos em operação de modo a alertar aos administradores e gestores da rede no momento em que se nota o funcionamento anormal ou avaria de tais componentes.

No presente trabalho, é feita a projecção e implementação de um sistema de monitorização de rede, na rede de computadores do Instituto Superior de Transportes e Comunicações (ISUTC). Apresentando a descrição da rede actual, as soluções existentes, vantagens e desvantagens do sistema, fases de implementação e análise dos resultados esperados.

1.2 Tema e sua delimitação

1.2.1 Tema

Projecto e implementação de um sistema de monitorização de rede no ISUTC.

1.2.2 Delimitação do tema

Projecto e implementação de um sistema de monitorização de rede, na rede de computadores do ISUTC para monitorizar os serviços de rede.

1.3 Objecto da investigação

No contexto da implementação de um sistema de monitorização de rede, o objecto da investigação é um sistema de análise.

1.4 Formulação do problema

O Instituto Superior de Transportes e Comunicações (ISUTC) possui uma rede de computadores em operação neste momento com o objectivo de partilhar os recursos e serviços de rede existentes como: acesso a Internet, partilha de ficheiros, impressoras, troca de mensagens instantâneas, correio electrónico e páginas *Web* internas que formam a sua intranet.

De modo a dar suporte aos serviços e recursos mencionados estão presentes na rede, 6 servidores que implementam os serviços da rede que são executados no meio lógico através da implementação de alguns protocolos da pilha de protocolos *TCP/IP*. Protocolos esses, que garantem a operação contínua e funcionamento da rede.

Durante o funcionamento da rede, em alguns momentos surgem problemas que causam a interrupção parcial ou total do funcionamento da rede, deixando assim, os utilizadores da rede sem acesso a alguns ou todos os recursos e serviços.

Por vezes, o Sector de Informática tem dificuldades em identificar estes problemas no momento em que ocorrem, sendo que na maioria das vezes são os utilizadores que reportam alguma dificuldade em aceder aos recursos ou serviços.

Deste modo surge a necessidade de uso de um sistema de monitorização de rede capaz de auxiliar na gestão e administração da rede.

Tendo este trabalho, a finalidade de projectar e implementar um sistema de monitorização de rede, pode-se questionar o seguinte:

Que mudanças positivas do ponto de vista de operação da rede, a implementação de um sistema de monitorização de rede poderá agregar a rede do ISUTC?

Com a implementação de um sistema de monitorização de rede, os administradores da rede do ISUTC poderão fazer um melhor acompanhamento no que diz respeito ao estado da infra-estrutura da rede e permitindo também que eles possam reagir prontamente aos problemas que possam surgir evitando que a rede fique com a sua operação totalmente interrompida.

Objectivos

Objectivo geral

Implementar um sistema de monitorização na rede de computadores do ISUTC.

Objectivos específicos

- Identificar os serviços de rede implementados;
- Identificar os problemas de rede existentes;
- Definir os sistemas de monitorização existentes;
- Escolher e implementar um sistema de monitorização.

1.6 Metodologia

Para a elaboração deste trabalho e posterior implementação do sistema, foram realizadas as seguintes actividades de modo a concretizar cada um dos objectivos específicos:

Identificar os serviços de rede implementados

De modo a identificar os serviços de rede implementados foi feito o levantamento de informações referentes aos serviços de rede implementados através de entrevistas abertas e não estruturadas. Estas entrevistas foram direccionadas aos administradores de serviços e infra-estruturas da rede do ISUTC. Com estas entrevistas foi possível obter a descrição dos serviços implementados bem como as suas funcionalidades.

Identificar os problemas de rede existentes

Para a identificação dos problemas de rede existentes mais frequentes, foi feito uma análise junto com os técnicos da assistência técnica e helpdesk do ISUTC, obtendo assim, com mais precisão, uma relação dos problemas que mais ocorrem e que são igualmente, os que mais interrompem o trabalho realizado pelos funcionários e as tarefas que os estudantes necessitam de realizar.

Definir os sistemas de monitorização existentes

Para definir os sistemas de monitorização existentes, foi realizada uma pesquisa bibliográfica, isto é, a consulta de livros e páginas da internet, que tratam do assunto.

Escolher e implementar um sistema de monitorização

Após uma análise exaustiva dos sistemas existentes e disponíveis, tomando em conta o desempenho, compatibilidade, vantagens, desvantagens e a relação custo benefício, foi escolhido um sistema a implementar. Para a sua posterior implementação foram definidos o ambiente de execução e as fases de implementação.

1.7 Justificação do tema

Os sistemas de monitorização de rede desempenham um papel muito importante no que diz respeito à gestão de redes de computadores, principalmente quando se trata de uma rede implementada numa empresa, pois qualquer problema que possa surgir e que não seja detectado a tempo e hora, pode de um certo modo trazer custos adicionais indesejáveis para empresa além de comprometer de forma significativa o funcionamento da empresa.

O ISUTC é uma instituição de ensino superior, que têm implementada uma rede de computadores com a finalidade de prover a partilha de recursos e informação aos seus utilizadores. No grupo dos utilizadores existem os estudantes, professores e funcionários da instituição. Os estudantes utilizam a rede para aceder a Internet para pesquisa de informação, para trocar correspondência através do correio electrónico, e acesso remoto dos seus ficheiros ou arquivos disponibilizados pelos professores. Os professores utilizam a rede para aceder a internet para preparar as matérias a leccionar, trocar correspondência através do correio electrónico, e partilhar informações com os estudantes. Os funcionários utilizam a rede para trocar a correspondência através do correio electrónico, acedem a Internet para obterem certas

informações acerca do trabalho a ser desenvolvido, partilhar informações e recursos de rede entre eles, como por exemplo impressoras. Neste momento a rede do ISUTC possui um total de 606 utilizadores dos serviços de rede da instituição dos quais 500 são estudantes.

Analisado o estado actual da rede de computadores do ISUTC quanto a sua dimensão medida pelo número de utilizadores, e pela importância dos serviços de rede que nela estão implementados, conclui-se que é de grande importância a utilização de um sistema com a finalidade de ajudar aos administradores na gestão da rede.

Para a implementação de um sistema de monitorização, o estudante terá que utilizar como base os conhecimentos adquiridos durante o curso que tratam das áreas de redes de computadores, protocolos de comunicação de redes, infra-estruturas de redes, programação e sistemas operativos.

1.8 Estrutura do trabalho

O presente trabalho está composto por 6 capítulos:

- Capítulo I – Introdução: refere-se a uma breve introdução do trabalho, esclarece os seus objectivos geral e específicos bem como a metodologia usada para atingir tais objectivos.
- Capítulo II – Marco teórico-conceitual da investigação: aborda todos os conceitos relacionados com o trabalho através de uma fundamentação teórica sobre os conceitos referentes ao trabalho e sobre as tecnologias usadas para a sua elaboração.
- Capítulo III – Marco contextual da investigação: centraliza-se na descrição da situação actual da rede do ISUTC e faz a descrição do sistema proposto bem como a sua implementação.
- Capítulo IV – Metodologia de resolução do problema e apresentação de resultados: apresenta os resultados obtidos da implementação e dos testes feitos ao sistema.
- Capítulo V – Conclusões e recomendações: refere-se as conclusões e recomendações sobre o trabalho.

CAPÍTULO 2 MARCO TEÓRICO-CONCEITUAL DA INVESTIGAÇÃO

Introdução

As redes de computadores actuais são compostas por uma grande variedade de dispositivos que devem se comunicar e compartilhar recursos. Na maioria dos casos, a eficiência dos serviços prestados está associada ao bom desempenho dos sistemas da rede. Para gerir esses sistemas e as próprias redes, um conjunto eficiente de ferramentas de monitorização automatizadas é necessário, sendo fundamental a utilização de técnicas padronizadas para a correcta representação e o intercâmbio das informações obtidas.

2.1 Gestão de Redes

A definição de Gestão de Redes depende do ponto de vista que se adopta. Em alguns casos envolve constantes monitorizações das actividades da rede utilizando um analisador de protocolo. Já em casos mais complexos há o envolvimento de uma base de dados distribuída e consultas aos dispositivos da rede, gerando gráficos em tempo real das mudanças ocorridas na topologia da rede e do seu tráfego. [L2].

Segundo Pinheiro (2006, p.1) "A Gestão de Redes pode ser definida como a coordenação (controlo de actividades e monitorização de uso) de recursos materiais (modems, *routers*, etc.) e ou lógicos (protocolos), fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade, tempos de resposta aceitáveis e segurança das informações".

A gestão de redes é constituída por três etapas, podendo essas etapas organizarem-se do seguinte modo:

- Colecta de dados – é um processo, em geral automático, que consiste na monitorização sobre os recursos a serem geridos;
- Diagnóstico – é um processo que consiste no tratamento e análise realizados a partir dos dados colectados. O computador de gestão executa uma série de procedimentos (por intermédio de um operador ou não) com o intuito de determinar a causa do problema representado no recurso gerido;
- Acção ou controlo – uma vez diagnosticado o problema, cabe uma acção, ou controlo, sobre o recurso, caso o evento não tenha sido passageiro (incidente operacional). [S1]

2.1.1 Metas para a Gestão

As principais metas de gestão a serem alcançadas são resumidas nos tópicos seguintes:

- *Maior disponibilidade dos recursos de rede:*

  A gestão da rede visa garantir uma maior disponibilidade dos dispositivos sendo geridos, através do uso constante de monitorização de indicadores, como falhas e desempenho, e ajustes através da função de controlo.

- *Redução dos custos operacionais da rede:*

  A redução de custos na rede pode ser feita com a monitorização e ajustes dos componentes da rede, bem como na escolha do modelo de gestão, centralizado ou distribuído, de forma a se adequar melhor à rede.

- *Aumento da flexibilidade de operação e integração:*

  Tecnologias de rede mudam constantemente. Com a adopção de padrões na gestão de rede é possível absorver tais tecnologias com custo mínimo.

- *Aumento da eficiência:*

  A eficiência geral da rede é aumentada quando metas como redução do custo operacional, aumento da disponibilidade dos recursos da rede são alcançadas.

- *Facilidade de uso:*

  A interface final para o administrador da rede é crítica para o sucesso de uma plataforma de gestão. A plataforma de gestão deve oferecer uma interface mais amigável possível, facilitando a análise dos dados colectados.

- *Segurança:*

  Algumas funções de gestão precisam de características de segurança. Pode-se fornecer a segurança em dois níveis: no nível de computador e de rede. A segurança no nível do computador consiste da protecção das informações nos sistemas de *softwares*, enquanto no nível de rede fornece esquemas de segurança para as informações que circulam na rede e para os nós sendo geridos. [L2].

2.1.2 Recursos geridos

A gestão de redes de computadores envolve a monitorização e o controlo de diferentes elementos de *hardware* e *software*, dentre os quais podem ser citados:

- Componentes de computadores, tais como dispositivos de armazenamentos, impressoras, etc.

- Componentes de interconexão e conectividade, tais como *routers*, concentradores *(hubs)*, comutadores *(switches)*, *APs*, etc.
- *Softwares* de aplicação e ferramentas de desenvolvimento. [L2].

As redes de computadores devem estar disponíveis o tempo todo para auxiliar as instituições, empresas e organizações a atingir objectivos como vendas, qualidade, rapidez e eficiência.

2.2 Gestão de redes *TCP/IP*

Com a crescente necessidade de gestão de redes, fez-se necessário que padrões para ferramentas fossem estabelecidos. Em resposta a esta necessidade surgiram dois padrões: família de protocolos *SNMP*[1] (protocolo padrão para gestão de redes *TCP/IP*[2]) e sistema de gestão *OSI*[3]. [S3]

- Família de Protocolos *SNMP*: o protocolo *SNMP* refere-se a um conjunto de padrões para gestão que inclui um protocolo, uma especificação de estrutura de dados, e um conjunto de objectos de dados.

- Sistemas de gestão OSI: refere-se a um grande conjunto de padrões de grande complexidade, que definem aplicações de propósito geral para gestão de redes, um serviço de gestão e protocolo, uma especificação de estrutura de dados, e um conjunto de objectos de dados. Este conjunto de protocolos é conhecido como *Common Management Information Protocol (CMIP)*. Pela sua complexidade, e pela lentidão do processo de padronização, este sistema de gestão não é muito popular.

2.2.1 Sistema de gestão de rede

Um sistema de gestão de rede defini-se como um conjunto de ferramentas integradas para a monitorização e controlo, que oferece uma interface única e que traz informações sobre o estado da rede podendo oferecer ainda um conjunto de comandos que visam executar praticamente todas as actividades de gestão sobre o sistema em questão.

[1] *Simple Network Management Protocol*
[2] Modelo de referência *TCP/IP*
[3] Modelo de referencia *Open Systems Interconnection (OSI)*

Arquitectura do sistema

A maioria das arquitecturas de gestão de redes utiliza a mesma estrutura básica e conjunto de relações. Dispositivos geridos, tais como computadores ou dispositivos de rede, executam um *software* que os habilita a enviar alertas quando algum problema é detectado. Recebendo esses alertas, as entidades de gestão são programadas para reagir executando uma ou várias acções, incluindo notificação aos operadores do sistema, adicionar ao histórico de eventos, desligamento do dispositivo, e tentativa de reparo automático.

Entidades de gestão também podem requisitar valores de certas variáveis às estações da rede. Essas requisições podem ser automáticas ou activadas pelo utilizador, mas o agente no dispositivo gerido responde a todas as requisições.

A arquitectura geral dos sistemas de gestão de redes *TCP/IP* apresenta quatro componentes básicos que são:

- os elementos geridos;
- as estações de gestão;
- os protocolos de gestão; e
- as informações de gestão ou *MIB*[4].

A estação de gestão serve de interface para o gerente humano num sistema de gestão de rede.

Os recursos a serem geridos são representados como objectos, e a colecção de objectos é referenciada como *MIB.*

Os elementos geridos são dotados de um programa chamado agente, que permite a monitorização e controlo do equipamento através de uma ou mais estações de gestão. Em princípio, qualquer dispositivo de rede (impressoras, *routers*, repetidores, *switches*, etc) pode ter um agente instalado. O agente de gestão responde as solicitações de informações e de acções da estação de gestão e deve também prover assincronamente informações importantes que não foram solicitadas por esta estação.

[4] *Management Information Base* (Base de Informações de Gestão)

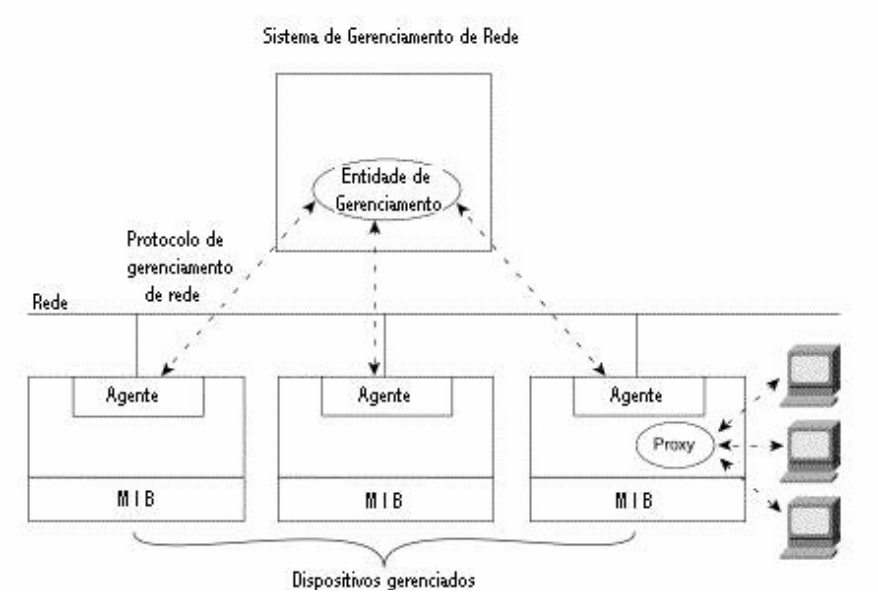


Figura 2.1 – Arquitectura de gestão da rede

Fonte: O Gerenciamento de Redes (p.1)[S9]

A forma de comunicação entre a estação de gestão e o agente é definido pelo protocolo de gestão de redes *TCP/IP*, o *SNMP*.

Simple Network Management Protocol

O *SNMP* é o protocolo de gestão recomendado para a gestão de redes *TCP/IP*, é um protocolo de gestão definido a nível da camada de aplicação, utilizando os serviços do protocolo de transporte *UDP*[5] para enviar suas mensagens através da rede. Sua especificação está contida no *RFC*[6] *1157*. Este protocolo é o centro do desenvolvimento da gestão *SNMP* e tem como premissa à flexibilidade e a facilidade de implementação, também em relação aos produtos futuros.

O *SNMP* é utilizado para obter informações de servidores *SNMP*, que são agentes espalhados em uma rede baseada na pilha de protocolos *TCP/IP*. Os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte *UDP* para enviar e receber suas mensagens através da rede.

Os cinco tipos de mensagens *SNMP* que são trocadas entre o gerente e o agente são:

[5] *User Datagram Protocol*
[6] *Request for Comments* (documento que descreve os padrões de cada protocolo da Internet)

- *get-request-UDP*: mensagem enviada pelo gerente ao agente solicitando o valor de uma variável;
- *get-next-request-UDP*: mensagem utilizada pelo gerente para solicitar o valor da próxima variável depois de uma ou mais variáveis que foram especificadas;
- *set-request-UDP*: mensagem enviada pelo gerente ao agente para solicitar que seja alterado o valor de uma variável;
- *get-response-UDP*: mensagem enviada pelo agente ao gerente, informando o valor de uma variável que lhe foi solicitado;
- *trap-UDP*: mensagem enviada pelo agente ao gerente, informando um evento ocorrido.

Além de ter sido projectado para operar sob *UDP*, um protocolo não orientado a conexão, o próprio *SNMP* também e um protocolo não orientado a conexão, sendo cada troca de mensagens uma transacção diferente entre o agente e a estação de gestão. Cada estação de gestão, como também o agente, devem implementar os protocolos *SNMP* e, por consequência, *UDP* e *IP*[7] para poderem se comunicar. Tal imposição exclui do processo de gestão dispositivos que não suportam parte dos protocolos *TCP/IP*, ou que, apesar de implementarem o *TCP/IP* para suportar suas aplicações, não desejam adicionar mais carga ao seu sistema com o suporte ao protocolo *SNMP*.

A gestão da rede através do *SNMP* permite o acompanhamento simples e fácil do estado, em tempo real, da rede, podendo ser utilizado para gerir diferentes tipos de sistemas. Esta gestão é conhecida como modelo de gestão *SNMP*, ou simplesmente, gestão *SNMP*. Por tanto, o *SNMP* é o nome do protocolo no qual as informações são trocadas entre a *MIB* e a aplicação de gestão como também é o nome deste modelo de gestão.

Os comandos *SNMP* são limitados e baseados no mecanismo de busca/alteração. No mecanismo de busca/alteração estão disponíveis as operações de alteração de um valor de um objecto, de obtenção dos valores de um objecto e suas variações.
A utilização de um número limitado de operações, baseadas em um mecanismo de busca/alteração, torna o protocolo de fácil implementação, simples, estável e flexível. Como

[7] *Internet Protocol (*Protocolo de Internet*)*

consequência reduz o tráfego de mensagens de gestão através da rede e permite a introdução de novas características.

O funcionamento do *SNMP* é baseado em dois dispositivos o agente e o gerente. Cada máquina gerida é vista como um conjunto de variáveis que representam informações referentes ao seu estado actual, estas informações ficam disponíveis ao gerente através de consulta e podem ser alteradas por ele. Cada máquina gerida pelo *SNMP* deve possuir um agente e uma *MIB*. [S2].

SNMPv2 e *SNMPv3*

Apesar do alto índice de aceitação, a implementação de protocolos e aplicações *SNMP* apresentaram deficiências, principalmente, com relação a segurança e a transferência eficiente de um grande número de informações do agente para o gerente. Além disso, o *SNMP* não se adequa a gestão de grandes redes de computadores, devido ao fato de apresentar limitações de desempenho para obtenção de requisições explícitas, e não dar suporte à comunicação gerente-gerente.

Durante o ano de 1993, foram publicadas 11 *RFC*s definindo revisões para o *SNMP* e dando início ao padrão *SNMPv2*, sendo o primeiro, o *RFC 1441*.

Esta série de revisões trouxe consigo grandes avanços que foram incorporados ao protocolo original. Tais avanços podem ser classificados de acordo com as seguintes categorias:

- Estrutura de informação;
- Primitivas de comunicação (*UDPs*);
- Comunicação gerente-gerente e gestão hierárquica;
- Segurança.

A estrutura de informação de gestão para o *SNMPv2* é mais elaborada, e eliminou ambiguidades nas definições dos objectos encontrados nas especificações anteriores.

Em relação às primitivas foram acrescentados dois novos *UDPs*:

- *get-bulk-request-UDP:* que permite que uma grande quantidade de informações possa ser transferida do agente para o gerente eficientemente;
- *inform-request-UDP*: que permite a um gerente enviar ou eventualmente solicitar informações a outro gerente.

A comunicação gerente-gerente, como também a gestão hierárquica, foram incorporadas ao protocolo com a introdução do novo tipo de mensagem, *inform-request;* e com a *SNMPv2-M2M MIB*, que é constituída por dois grupos: um grupo de alerta e um grupo de eventos.

No aspecto da segurança, o *SNMPv2* acrescentou ao protocolo novos conceitos e serviços que trouxeram mais segurança ao protocolo. Os conceitos incluídos foram: o conceito de visão de *MIB* definido em termos de sub-árvores, restringindo o acesso a porções predefinidas da *MIB*; e o conceito de contexto, que é uma colecção de objectos e seus respectivos agentes, e a especificação dos privilégios envolvidos. [S4].

O *SNMPv3* incluiu implementação na segurança ao protocolo como, autenticação e controle de acesso o que garante a confidencialidade e integridade. Em 2004 a *IETF*[8] declarou o *SNMPv3* definido pelas *RFC 3411* e *RFC 3418* como a versão padrão do *SNMP*, e normalizou o *SNMPv3* como *full Internet standard*, que é o nível mais alto para um *RFC*, e considera obsoletas as primeiras versões, as designando de históricas.

Na prática, as implementações do *SNMP* oferecem suporte para as múltiplas versões *(RFC 3584)*, tipicamente *SNMPv1*, *SNMPv2* e *SNMPv3*.

Management Information Base

A *MIB* é o conjunto dos objectos geridos, que procura abranger todas as informações necessárias para a gestão da rede, possibilitando assim, a automatização de grande parte das tarefas de gestão.

Ela pode ser caracterizada como uma base de dados activa, o que possibilita que os valores das suas variáveis sejam, não só recuperados, como também alterados.

Cada agente deve manter sua própria instância da *MIB*, relacionada com os objectos que estão sendo geridos sob o seu domínio. O *RFC 1213*, define um conjunto de variáveis utilizadas para a monitorização e o controlo de redes *TCP/IP*.

Para cada novo dispositivo a ser gerido, que não tenha sido previsto a sua gestão, é necessário que seja definido um conjunto de novas variáveis, estendendo assim, a *MIB-II* original.

[8] *Internet Engineering Task Force*

Estrutura da MIB

A estrutura da MIB e a identificação dos objectos geridos são definidos no padrão chamado *Structure of Management Information* (*SMI*), encontrados no *RFC 1155*. As definições são feitas utilizando-se um pequeno conjunto de características e elementos ASN.1[9].

Associado a cada um dos objectos da *MIB*, está o seu identificador, que nomeia este objecto. Um identificador de um objecto, é um identificador único, que consiste numa sequência de inteiros conhecidos como sub-identificadores. A sequência, lida da esquerda para a direita, define a localização deste objecto na estrutura de árvore da *MIB*. Esta identificação segue uma estrutura hierárquica, cuja convenção também serve para identificar os tipos dos objectos.

O documento *SMI*, define quatro nós abaixo do nó Internet:

- *directory*: esta sub-árvore é reservada para o uso futuro do X.500l;
- *mgmt*: esta sub-árvore é utilizada para os objectos geridos definidos em documentos *IAB* aprovados;
- *experimental*: esta sub-árvore é utilizada para identificadores de objectos geridos usados em experiências na Internet;
- *private*: esta sub-árvore está reservada para a utilização de identificadores de objectos geridos definidos unilateralmente, por exemplo, por fabricantes que desejem ter seus próprios objectos. [S3]

Tipos de dados

O *SNMP* utiliza apenas um pequeno conjunto de diferentes tipos de dados, classificados em tipos universais e tipos de aplicação.

[9] *Abstract Syntax Notation One,*

Tipos universais

Estes são os tipos permitidos para definirem objectos da *MIB*. Eles são baseados na classe UNIVERSAL:

1. *INTEGER* (UNIVERSAL 2);
2. *OCTET STRING* (UNIVERSAL 4);
3. *NULL* (UNIVERSAL 5);
4. *OBJECT IDENTIFIER* (UNIVERSAL 6);
5. *SEQUENCE*, *SEQUENCE OF* (UNIVERSAL 16);

Tipos de aplicação

Os tipos de aplicação são:

1. *DisplayString*: uma *string*[10] de 0 ou mais octetos. Cada variável deste tipo na *MIB-II*, não deve possuir mais de 255 caracteres;
2. *IpAddress*: este tipo é um *OCTET STRING* de tamanho 4, um para cada octeto do número *IP*;
3. *PhysAdress*: um *OCTET STRING* que especifica o endereço físico;
4. *Counter*: um inteiro não negativo, que só pode ser incrementado e não decrementado;
5. *Gauge*: um inteiro não negativo, que pode ser tanto incrementado como decrementado;
6. *TimeTicks*: um inteiro não negativo, que armazena o tempo em centenas de segundos, a partir de alguma época.

Tipos de sistemas de gestão de rede

Existem dois tipos de sistemas de gestão que estão condicionados a topologia de rede empregue, que são:

- Sistema de gestão centralizado – deve possuir pelo menos uma estação de gestão. Os problemas com os modelos centralizados de gestão de redes tornam-se mais críticos na proporção em que a rede cresce.

[10] Cadeia de caracteres

- Sistema de gestão distribuído – possui duas ou mais estações de gestão. Permite que o trabalho seja feito de forma hierárquica, ou seja, cada nó é responsável por determinado tipo de actividade gestão.

Nas estações de gestão encontramos o *software*[11] gerente, responsável pela comunicação directa desta estação com os agentes nos elementos geridos. As operações de monitorização e de controlo são feitas através dos protocolos de gestão.

Gerentes e agentes podem trocar tipos específicos de informações, conhecidas como informações de gestão. Tais informações definem os dados que podem ser utilizados nas operações do protocolo de gestão.

O sistema de gestão de uma rede é integrado e composto por uma colecção de ferramentas para monitorar e controlar seu funcionamento. Uma quantidade mínima de equipamentos separados é necessária, sendo que a maioria dos elementos de *hardware* e *software* para gestão está incorporada aos equipamentos já existentes.

Distribuição da gestão

Como mencionado, um sistema de gestão consiste de alguns ítems de *hardware* e *software* adicionais, implementados entre os equipamentos de rede existentes.

O *software* usado para auxiliar o gestão da rede é instalado em servidores, estações e processadores de comunicação, tais como, roteadores, concentradores de acesso e *switches*. Ele é projectado para oferecer uma visão de toda a rede como uma arquitectura unificada, com endereços e rótulos associados a cada ponto da rede e atributos específicos de cada elemento e *link*[12] conhecido do sistema de gestão.

Com o crescimento das redes de computadores, em tamanho e complexidade, sistemas de gestão baseados em um único gerente são inapropriados, devido ao volume das informações que devem ser tratadas e que podem pertencer a localizações geograficamente distantes do gerente. Evidencia-se, então, a necessidade da distribuição da gerência na rede, através da divisão das responsabilidades entre gerentes locais que controlem domínios distintos e da expansão das funcionalidades dos agentes.

[11] Programa de computador
[12] Meio de comunicação

Os modelos de gestão diferenciam-se nos aspectos organizacionais envolvendo a disposição dos gerentes na rede, bem como no grau da distribuição das funções de gestão. Cada gerente local de um domínio pode prover acesso a um gerente responsável[13] local e ou ser automatizado para executar funções delegadas por um gerente de mais alto nível, geralmente denominado de *NOC*[14]. O *NOC* é responsável por gerir os aspectos inter-domínios, tal como um enlace que envolva vários domínios, ou aspectos específicos de um domínio, devido à inexistência de gerente local.

Configuração do sistema de gestão

Na representação da arquitectura básica de um sistema de gestão de rede, cada nó da rede possui uma colecção de *softwares* dedicados à tarefa de gestão da rede.

Pelo menos um servidor da rede é designado para exercer a função de servidor de gestão da rede. O servidor de gestão da rede possui uma colecção de *softwares* denominados de *Network Management Application* (*NMA*). A *NMA* inclui uma interface de operador para permitir que um utilizador autorizado faça a gestão da rede. A *NMA* responde aos comandos do operador, mostrando informações e/ou enviando comandos para os agentes através da rede.

Outros nós que fazem parte do sistema de gestão de rede incluem um módulo agente que responde às solicitações do servidor de gestão. Os agentes são implementados em sistemas finais que suportam aplicações de utilizadores finais, bem como em nós que fornecem serviços de comunicação, tais como, roteadores e controladores de acesso remoto.

Para manter a alta disponibilidade de gestão, dois ou mais servidores são usados. Em condições normais, um deles é usado para o controle, enquanto os outros ficam colectando estatísticas ou em estado de espera. No caso de falha daquele que está sendo utilizado para controlo, outro poderá substituí-lo.

[13] pessoa que interage com o sistema de gestão
[14] *Network Operation Center* (Centro de Operações de Rede)

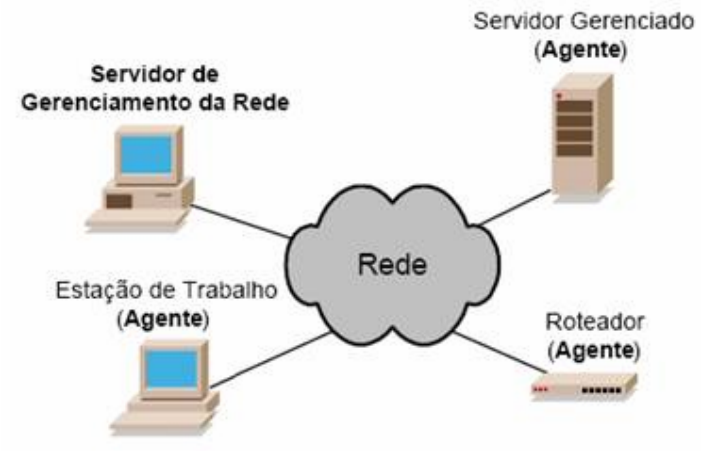


Figura 2.2 – Arquitectura do sistema de gestão de rede
Fonte: Pinheiro (p.1)[S1]

2.3 Sistema de Monitorização de Rede

O termo monitorar a rede descreve o uso de um sistema que contém um conjunto de ferramentas que constantemente fazem o acompanhamento de uma rede de computadores para a detecção de falhas ou lentidão dos componentes de rede, e que notifica o administrador da rede, seja por *e-mail*[15], *pager*[16] ou outros alarmes em caso de interrupção do funcionamento desses componentes.

Os sistemas de monitorização de rede são sistemas que têm como função o controlo permanente sobre a operação e funcionamento de componentes de uma rede de computadores, sendo esses componentes computadores (estações de trabalho e servidores), *switches* e *routers*. Esses sistemas permitem também monitorar a infra-estrutura de rede e aplicações de rede.

O objectivo principal do uso de um sistema para monitorar uma rede é auxiliar os administradores e gestores da infra-estrutura da rede no acompanhamento contínuo do funcionamento da rede, focalizando o controlo de possíveis falhas ou comportamentos anormais que os componentes da rede podem vir a apresentar.

[15] Correio electrónico
[16] Rádio mensagem

2.3.1 Parâmetros de avaliação das ferramentas

Antes de se efectuarem quaisquer comparações, é importante que se saiba que parâmetros utilizar nessa comparação, tendo-se em conta a finalidade e os objectivos do projecto. Aqui são delineados exactamente os parâmetros avaliados pelo autor na escolha da ferramenta ideal para implementar este mesmo projecto.

Existem dois modelos de gestão de redes, fundamentais na criação ou escolha de ferramentas de monitorização, que foram desenvolvidos em 1996. A *International Telecommunication Union* (*ITU*), introduziu nessa altura o modelo *Telecommunications Management Network* (*TMN*) [S5], constituído por quatro camadas lógicas: *Business Management, Service Management, Network Management* e *Element Management*. Mais tarde, em 1997, publicou um modelo que consistia na especificação da 3ª camada, *Network Management*, chamada modelo *FCAPS* que é constituído pelas seguintes categorias [S6]:

- Gestão de Falhas (*Fault Management*) – verificação da disponibilidade de dispositivos remotos e de serviços públicos;
- Gestão de Configurações (*Configuration Management*) – alteração de configurações respectivas aos dispositivos que se monitorizam;
- Relatório de Actividades (*Accounting*) – manutenção de relatórios com informação respectiva a quem faz o quê na rede;
- Gestão de Desempenho (*Performance Management*) – recolha de dados e sua posterior apresentação gráfica;
- Segurança (*Security*) – controlo ao acesso aos dados disponibilizados pela aplicação e segurança na comunicação entre estações de gestão e agentes.

Estes dois modelos são frequentemente utilizados como listas de funcionalidades a implementar por parte de quem desenvolve ferramentas de monitorização, e farão parte da análise aqui apresentada.

Em relação à segurança, o terminal de monitorização pode ser definido, na perspectiva dos *hackers*[17], como uma *backdoor*[18] para a rede onde se deseja penetrar. Muitas vezes, estes

[17] são indivíduos que elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas.
[18] Falha de segurança que pode existir em um programa de computador ou sistema operativo

terminais têm acesso a redes através de *firewalls*, sendo-lhes permitido obter informação acerca dos recursos que estão a monitorar. Porém essa informação pode ser utilizada para atacar a rede em causa. Essa conveniência torna os terminais de monitorização num sistema alvo, pois uma vez comprometida a segurança nestes, será mais fácil comprometer a segurança da rede que se deseja atacar. Como exemplo, temos o caso em que o administrador utiliza chaves *Secure Shell*[19] (*SSH*) partilhadas.

Outro aspecto importante consiste na verificação da autenticidade das mensagens recebidas. Um *hacker* pode facilmente entregar informação falsificada à estação de monitorização fazendo com que esta apresente dados estatísticos falsos, e despolete eventos com base em notificações falsas, o que pode ser um enorme problema caso tenham-se eventos que, por exemplo, reiniciem serviços, ou reiniciem o sistema (*cycling power*)[20], ou ainda que enviem *sms's* falsos causando deslocações desnecessárias a administradores.

Outro potencial problema, consiste na confidencialidade das mensagens trocadas entre a estação que faz a gestão e os clientes. Isto é importante pois existe a possibilidade de um *hacker* fazer *sniffing*[21] à rede e obter informação que lhe ajude a efectuar outros ataques à rede ou aos sistemas em causa. Esta confidencialidade é obtida através da cifra dos canais de comunicação. Caso isto não seja implementado, corre-se o risco de se sofrerem ataques, como por exemplo, se um *hacker* souber a carga de processador e o número de utilizadores dum sistema, utilizados ao longo de um dia, fica automaticamente a saber quando poderá invadir esse sistema e utilizar os recursos por este disponibilizado sem que ninguém se aperceba do facto.

Existem, no entanto, duas ameaças das quais esses sistemas não se deverão proteger: ataques DoS e análise de tráfego. Os ataques de DoS resultam na impossibilidade de obtenção de dados por parte da estação de gestão, dada a falta de disponibilidade resultante deste tipo de ataques. Porém, essa indisponibilidade é praticamente impossível de distinguir de falhas de rede, que deverão ser familiares a qualquer administrador, e que deverão ser tidas em conta na

[19] protocolo para login remoto seguro
[20] é o acto de desligar e ligar novamente um equipamento, geralmente um computador
[21] interceptar e registrar o tráfego de dados em uma rede de computadores

implementação destas ferramentas. Quanto à análise de tráfego, o tráfego de dados é feito de forma periódica, pelo que a análise desse fluxo de tráfego não tem significado algum.

Dados todos estes problemas, torna-se óbvio que a segurança é um factor crítico na escolha do sistema a utilizar, sendo este consequentemente o elemento de maior peso nessa escolha. Alerta-se ainda para o facto de, por muito seguro que seja o sistema, se a segurança da rede onde este se executa não estiver garantida, de nada servirá o acréscimo que a segurança do sistema irá trazer.

CAPÍTULO 3 MARCO CONTEXTUAL DA INVESTIGAÇÃO

Neste capítulo é abordado o caso de estudo. É nele apresentado uma visão geral da rede do ISUTC, analisando seu estado actual, elementos existentes, topologia da rede, arquitectura e serviços existentes.

3.1 Estado actual da rede do ISUTC

O Instituto Superior de Transportes e Comunicações (ISUTC) é uma instituição privada de ensino superior em Moçambique vocacionada para a formação de quadros superiores nas áreas de conhecimento ligadas aos transportes e comunicações e suas envolventes, incluindo as tecnologias, a gestão e a economia, em particular as tecnologias de informação e comunicação, os transportes, a logística e distribuição, e gestão.

Os estatutos do ISUTC o consagram como sendo um centro de criação e difusão da ciência e da tecnologia, exercidas nos domínios do estudo da docência, da investigação e da prestação de serviços, em harmonia com os desígnios da identidade nacional e do desenvolvimento da comunidade nacional e internacional.

A rede de computadores do ISUTC, foi implementada com o propósito de fornecer serviços de rede de âmbito educacional e de âmbito operacional para o funcionamento da mesma.

No âmbito educacional, a rede foi projectada de modo a prover serviços para que os estudantes e docentes possam ter acesso as tecnologias de informação e comunicação com o objectivo do aprendizado. É com estas tecnologias que por exemplo os estudantes fazem a pesquisa de informações na Internet para estudos e realização de trabalhos, fazem uso do correio electrónico de modo a trocar a correspondência, e guardem ficheiros e arquivos de forma segura para uso posterior dentro da instituição. Os docentes por sua vez, acedem a Internet para colectar informações que servirão de base para a preparação das matérias das aulas a leccionar e fazem uso do correio electrónico para enviar informações sobre aulas, avaliações assim como forma de comunicação à distância com os estudantes.

No âmbito operacional para o funcionamento da instituição, a rede de computadores provê serviços aos órgãos administrativos que são nomeadamente, a Secretaria Académica, o Centro de Documentação (Cedoc), a Transcom, o Sector Pedagógico e o Laboratório Informático de

Ensino Auto Aprendizagem e Avaliação (LIMEAA). Nos órgãos mencionados é através da rede que são por exemplo enviadas/recebidas correspondências, impressos documentos e partilhadas informações.

3.1.1 Elementos de rede

A rede possui elementos de rede que desempenham um papel específico durante o seu funcionamento quando se encontram conectados a rede. Os elementos presentes na rede são:

- computadores (ou estações de trabalho);
- *routers* (roteadores);
- *switches* (comutadores);
- impressoras de rede;
- servidores.

As estações de trabalho são utilizadas pelos estudantes, docentes e funcionários, e é através delas que são acedidos aos serviços de rede implementados na infra-estrutura da rede.

Os *routers* são os dispositivos de interconexão que servem para interligar pelo menos duas redes, geralmente duas *LANs* ou *WANs* ou uma *LAN* e a rede do seu *ISP*[22]. Os *routers* encaminham pacotes de dados entre redes e são instalados em lugares onde duas ou mais redes se conectam. [S7]. Neste caso, o *router* interliga a rede interna do ISUTC com o provedor de serviços de internet TV Cabo.

Os *switches* ou comutadores são dispositivos que interligam vários computadores num *LAN*. Tecnicamente os *switches* operam na camada 2 (enlace de dados) do modelo *OSI*. [S9].

Os *switches* têm a função de interligar todos os computadores, servidores e impressoras presentes na rede.

As impressoras de rede são impressoras que possibilitam ser usadas por vários utilizadores da rede independentemente da sua localização física dentro da instituição.

Os servidores são as máquinas responsáveis pela disponibilização dos serviços de rede na instituição.

[22] Provedor do Serviço de Internet (*Internet Service Provider*)

3.1.2 Topologia de rede

Sendo utilizados os *switches* e *routers* dentro da rede de modo a possibilitar a interconexão dos elementos da rede, estes possibilitaram a implementação de uma topologia de rede que melhor se adequou a disposição física dos computadores presentes na instituição levando em conta a estrutura do edifício onde a instituição está instalada. A rede está implementada utilizando a topologia de rede estrela estendida.

3.1.3 Arquitectura de rede

Seguindo as distribuições das salas de aulas e laboratórios de trabalho existentes, foram implementadas diferentes arquitecturas de rede. Em alguns departamentos foi implementada a arquitectura *Fast Ethernet* e em outros *Gigabit Ethernet*, sendo suportadas pelo uso de meios de transmissão com fio utilizando o padrão de rede 802.3 que utiliza o cabo de par trançado de cobre, e meios de transmissão sem fio utilizando o padrão de rede *Wi-Fi* 802.11g.

3.1.4 Serviços existentes

Os serviços de rede que estão implementados e em uso são nomeadamente:

- Transferência de ficheiros – utilizando um servidor *FTP*;
- Acesso remoto – utilizando um servidor de *VPN* e *SSH*;
- Acesso a Internet – utilizando um servidor proxy;
- Correio electrónico (E-mail) – utilizando um servidor *SMTP*, *POP*, *IMAP e* Webmail;
- Páginas de Internet – utilizando um servidor *Web*;
- Controlador de domínio;
- Repositório de ficheiros – utilizando um servidor de arquivos;
- Mensagens instantâneas (Chat);
- Resolução de nomes de domínio – utilizando um servidor *DNS*;
- Atribuição de endereço dinâmico – utilizando um servidor *DHCP*;
- Backups;
- Bases de dados – utilizando um servidor de base de dados;

CAPÍTULO 4 METODOLOGIA DE RESOLUÇÃO DO PROBLEMA E APRESENTAÇÃO DE RESULTADOS

4.1 Comparação das ferramentas existentes

Já tendo sido feita análise ao protocolo de gestão de rede *SNMP*, a seguir faz-se uma análise as ferramentas Nagios [S9], OpenNMS [S10], Cacti [S11] e outras ferramentas.

4.1.1 OpenNMS

O OpenNMS endereça as camadas *Service Management* e *Network Management* do modelo *TMN* e endereça igualmente todo o modelo *FCAPS*, com especial ênfase à gestão de falhas e gestão de desempenho. A gestão de falhas é feita recorrendo ao *polling*, à recepção assíncrona de mensagens, como é o caso de *SNMP traps*, e recorrendo a *thresholds* comparando-os a dados de desempenho. A gestão de desempenho é feita recorrendo a protocolos como o *SNMP* e à comunicação com agentes como o *NSClient*. Quanto à gestão de configurações esta é feita através da *WebUI*. O relatório de actividades não é apresentado na parte gráfica mas pode ser enviado a estações externas que queiram processar esses dados.

Finalmente, em relação à segurança, esta é suportada:

- através da integração do *SNMPv3*;
- através do controlo local ou remoto a acessos à interface gráfica;
- através da integração com os sistemas de detecção de intrusões Snort e avaliação de vulnerabilidades Nessus.

A próxima aplicação em análise é o Nagios e consiste numa das melhores soluções *Open Source* para monitorar sistemas remotos, reconhecida principalmente pela sua flexibilidade e estabilidade.

4.1.2 Nagios

O Nagios consiste numa aplicação de monitorização de sistemas e de redes especializada, em termos do modelo *FCAPS*, na área de gestão de falhas. Essa monitorização é flexível e versátil devido à existência de ficheiros de configuração e à possibilidade de não só se poderem utilizar *plugins* diversos já existentes, como também criar novos de acordo com as necessidades do utilizador. Pode-se utilizar esta aplicação para monitorar serviços de rede, como a disponibilidade de servidores *POP*, *SMTP* e *HTTP*, e também pode-se-lhe utilizar

para monitorar recursos na máquina local ou em máquinas remotas, como a carga do processador e espaço disponível no disco rígido. Esta aplicação, na verdade, consiste apenas num *daemon*[23] que gere o processo de monitorização. A recolha dos dados, para posterior processamento por parte do Nagios, é feita por pequenas aplicações conhecidas por *plugins*, que retornam os dados ao *daemon* em causa. As máquinas e serviços de rede monitorizados pelo Nagios são todos definidos através dos ficheiros de configuração que contêm informação como os contactos que deverão ser informados de possíveis falhas, informação dos *hosts* a serem monitorizados, comandos existentes, sendo que um comando consiste na definição de que *plugin* deverá ser executado e dos respectivos parâmetros, e a definição de serviços que consistem na associação do *host* a ser monitorizado, do comando a ser executado, dos contactos a serem informados em caso de alertas, e outras informações necessárias a essa monitorização como, por exemplo, o número máximo de tentativas.
Em relação aos *outputs*, o Nagios traz uma interface *Web* integrada, que deve ser integrada à instalação local do *Apache*[24]. É possível também verificar informação de estado consultando o ficheiro de *log*[25].

Quanto à segurança, a confidencialidade, integridade e autenticidade obtêm-se através da utilização do protocolo *Secure Socket Layer* (*SSL*). Porém existem aspectos que requerem alguma ponderação por parte do administrador, como é o caso da monitorização remota, onde a ferramenta oficial é o *Nagios Remote Plugin Executor* (*NRPE*), sendo que a outra possibilidade consiste na utilização do *SSH*. Ambas apresentam as mesmas vantagens, contudo cada uma tem uma desvantagem. O *NRPE* abre mais uma porta *TCP*, o que vai contra o minimalismo desejado do ponto de vista de segurança, e o *SSH* consome maior carga de processador, problema esse que se agrava com o número de ligações abertas simultaneamente. Seguem-se alguns dos mais importantes exemplos de recomendações dadas na documentação oficial:

- Utilização de um terminal dedicado: isto reduz o risco de outras aplicações serem comprometidas e, através delas, se comprometer todo o sistema;
- Não executar o Nagios como utilizador *root*: o Nagios não necessita dos privilégios associados a esse utilizador para se executar, e não se executando nessa conta diminui-

[23] Representação de um programa em execução na memória
[24] Servidor *Web*
[25] Registos de execução de um programa

se o número de problemas que poderão ser causados por um *hacker* que se apodere da máquina;

- Restringir o acesso ao directório configurado como *check_result_path*: nesse directório, indicado no ficheiro de configuração principal do Nagios, só deverá ter acessos de leitura e escrita, o utilizador *nagios*, pois nela são armazenados os dados retornados pelos *plugins* temporariamente, antes de serem processados. Caso o acesso a essa directoria não seja vedada, poder-se-ão ter os mesmos problemas associados à falta de autenticidade e confidencialidade, causados por outros utilizadores do mesmo terminal;
- Restringir o acesso ao ficheiro configurado como *External Command File*: esse ficheiro, indicado no ficheiro de configuração principal do Nagios, funciona como um *buffer FIFO*, onde aplicações externas (exemplo *CGI's*) podem alterar o processo de monitorização em funcionamento, como por exemplo: forçando verificações de serviços de forma a que *sniffers* sejam postos em execução; alterando comandos, ou seja, alterar o *plugin* chamado e/ ou os parâmetros a ele associados; e através do cancelamento temporário de notificações;
- Proteger o acesso aos agentes remotos: como agentes remotos entendem-se aplicações como o já indicado *NRPE*, que consistem em pontes que fazem a comunicação entre os *plugins* e o Nagios. Outro exemplo seria a aplicação que faz a ponte entre o Nagios e sistemas Windows, que é o *NSClient*. Essa protecção deve ser aplicada pois não se quer que todos tenham acesso à informação disponibilizada por esses agentes remotos;
- Assegurar a confidencialidade dos canais de comunicação existentes entre o Nagios e os agentes remotos.

Na secção seguinte, analisa-se a aplicação Cacti que consiste numa excelente ferramenta de análise de desempenho.

4.1.3 Cacti

O Cacti consiste numa aplicação especializada na área de monitorização de desempenho, sendo uma muito boa escolha para quem deseja monitorar o desempenho de dispositivos remotos. Esta aplicação faz a recolha, o armazenamento, e a apresentação gráfica de dados inerentes ao desempenho de um dado dispositivo como, por exemplo, a carga de CPU, quantidades de memória ocupadas, ou larguras de banda consumidas numa interface.

O Cacti é constituído por uma interface gráfica, que utiliza a tecnologia *PHP*, para consultar uma base de dados MySQL, gerida também pelo Cacti. A informação é inserida, nessa base de dados, utilizando uma ferramenta denominada *RRDTool* (*Round Robin Database Tool*) que consiste numa ferramenta que armazena e apresenta dados que se alteram com o passar do tempo, como são os casos da temperatura numa sala de servidores ou da largura de banda consumida numa interface. Por sua vez, o *RRDTool* utiliza o conjunto de aplicações *SNMP*, contidas no pacote net-snmp, para a recolha dos dados a armazenar na base de dados. Isto tudo significa que os seguintes softwares são cruciais na instalação do Cacti:

- net-snmp: responsável pela recolha de dados;
- *RRDTool*: responsável pelo armazenamento;
- Apache *server* (httpd): servidor *Web*;
- MySQL (*server*): base de dados onde serão armazenados os dados;
- *PHP*: linguagem utilizada pela interface *Web* para consulta dos dados a apresentar.

O maior poder desta aplicação consiste na representação gráfica de dados que variam com o tempo. A facilidade em gerar e gerir gráficos, como os de desempenho, é amplamente reconhecida. Outra grande funcionalidade é a gestão de utilizadores, que permite ao administrador criar vários utilizadores, da interface, atribuindo a cada um diferentes níveis de permissões, fazendo com que estes tenham acesso a diferentes gráficos com informações distintas., visto que essas permissões podem ser especificadas em relação a cada gráfico.

Com o aumento do número de dados a recolher, o *poller*, ou seja, o *script* responsável pela recolha e armazenamento dos dados, começa a ter problemas de desempenho. Para solucionar este problema foi desenvolvido um *poller* chamado *Spine*, escrito utilizando a linguagem C, de forma a torná-lo mais eficiente, não só pelo código nativo, mas também pelo facto de este tomar partido de *threads* do sistema operativo (*pthreads*).

Uma das grandes falhas desta aplicação consiste no facto desta não conter a funcionalidade de notificar administradores quando os valores de um determinado gráfico saem dos limites especificados por um *threshold.*

A nível de segurança, esta aplicação tem suporte completo ao protocolo *SNMPv3.*

4.1.4 Outras aplicações

Existem inúmeras ferramentas de gestão/monitorização todos com o mesmo objectivo de monitorar e desencadear acções em dispositivos remotos em resposta à própria monitorização. Muitos especializam-se em certas áreas do modelo *FCAPS*, como já vimos, e outros tentam abrangi-los ao máximo. É importante deixar claro que as ferramentas aqui apresentadas não são as únicas, mas sim as melhores nas suas áreas de acordo com a avaliação do autor deste trabalho.

Como exemplo, tem-se o *Hobbit*, inspirado no *Big Brother*, que consiste num monitor centralizado que recebe dados de *softwares* instalados nas máquinas que se desejam monitorar. Porém, este não fornece tantas funcionalidades quanto o Nagios, por exemplo. Outra aplicação de monitorização é o *Monit* que, por sua vez, consiste numa ferramenta destinada a uma utilização mais modesta, tipicamente nos próprios sistemas que se desejam monitorar. Esta é particularmente conhecida pela sua muito boa integração com o *init* e os *rc-scripts*, o que lhe confere a capacidade de reiniciar serviços que poderão ter falhado.

Finalmente, têm-se várias outras aplicações cuja única funcionalidade consiste na interpretação de mensagens *SNMPv3*.

4.1.5 Conclusão

Com base na análise aqui feita, fica claro que não existe uma ferramenta que simplesmente se caracterize como sendo a melhor de todas. A conclusão, a que se chega, é a de que, com base nas características aqui apresentadas, fica a cargo de cada administrador escolher a solução que melhor lhe sirva. O OpenNMS é a aplicação mais completa, detentora das capacidades de analisar a disponibilidade de dispositivos remotos, alterar a configuração desses dispositivos conforme as conclusões chegadas a partir da própria monitorização, descoberta automática de dispositivos de rede, analisar o desempenho desses dispositivos demonstrando os resultados em gráficos intuitivos, e com suporte ao protocolo *SNMPv3*.

Por outro lado, temos dois especialistas, o Nagios e o Cacti. O Nagios especializa-se na monitorização de dispositivos remotos suportando, não só a comunicação via SNMP, mas também toda a flexibilidade e personalização proveniente das capacidades dos *plugins* que podem ter inúmeras utilidades não suportadas pelo *SNMP*. Essa especialização não significa a falta de suporte às outras funcionalidades, pois o Nagios também tem excelente suporte a

nível de segurança, tanto na utilização do *SNMPv3* como na comunicação com os respectivos agentes, tem toda a capacidade de alterar a configuração de dispositivos remotos dada pelo *SNMP* e tem excelente suporte para notificações.

Por último tem-se o Cacti, especializado na análise de desempenho, capaz de ler informação contida, não só em bases de dados MySQL como também, em ficheiros no formato RRD *files*. Ao contrário do Nagios, o Cacti, apenas contém a funcionalidade onde se especializa. Isto tudo resume-se na tabela abaixo.

Ferramentas e Parâmetros	*Nagios*		*OpenNMS*		*Cacti*	
	Avaliação	*Notas*	*Avaliação*	*Notas*	*Avaliação*	*Notas*
F	Melhor	Notificações flexíveis, verificações directas e indirectas	Bom	Notificações	Mau	-
C	Excelente	*SNMP*, expansível a aplicações próprias	Bom	*SNMP*	Mau	-
A	Bom	Delineamento da rede	Excelente	Delineamento da rede	Mau	-
P	Bom	MRTG	Bom	*RRDTool*	Melhor	*RRDTool*, Spine
S	Melhor	*SNMPv3*, *SSL/TLS*, controlo de acesso	Bom	*SNMPv3*, controlo de acesso	Bom	*SNMPv3*
Média	Excelente		Bom		Bom	

Tabela 4.1 - Principais diferenças entre as ferramentas avaliadas

Fonte: Autor

Feita a análise descrita na tabela acima, o autor conclui que o Nagios melhor se adequa aos propósitos de instalação de um sistema para monitorizar, dando maior flexibilidade a monitorização o que permite endereçar problemas específicos a rede do ISUTC.

4.2 Implementação do sistema

4.2.1 Arquitectura proposta

De acordo com a disposição lógica dos servidores presentes na rede, é proposta a seguinte arquitectura:

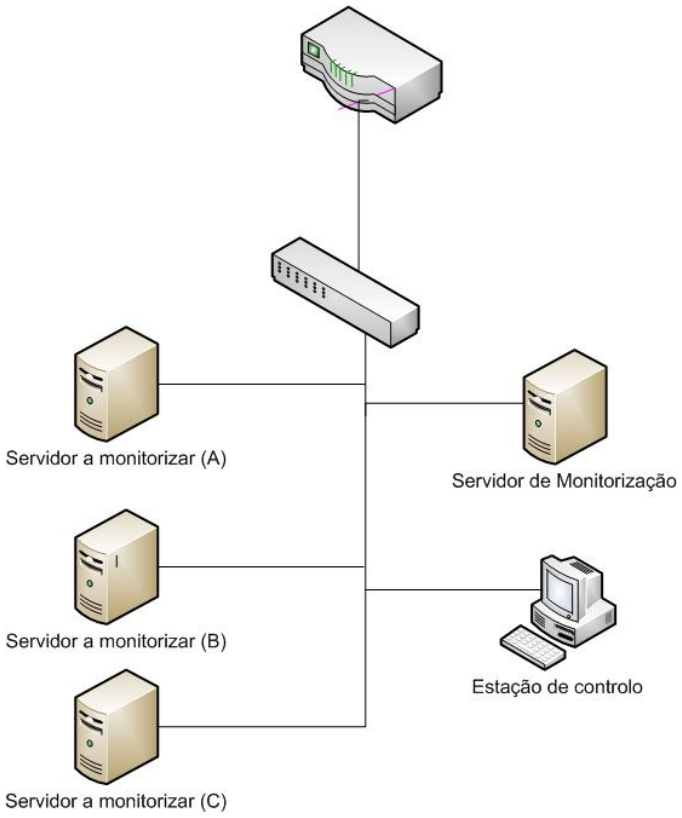


Figura 4.1 – Arquitectura de monitorização
Fonte: Autor

Tendo a rede, sido implementada com suporte a topologia de estrela estendida, e todos os computadores pertencendo ao mesmo domínio de colisão torna-se conveniente o uso desta arquitectura.

O servidor de monitorização é o servidor no qual o sistema estará implementado, possuindo assim as ferramentas necessárias para monitorizar os servidores que possuem os serviços.

Os servidores a serem monitorizados possuem os serviços de rede que estão disponíveis na rede para os seus utilizadores.

A estação de controlo servirá para visualizar e gerir o sistema de monitorização que estará no servidor de monitorização.

É importante realçar o facto de, nesta arquitectura, ser possível expandir a implementação do servidor de monitorização para vários servidores, com possíveis comunicações de estado entre eles. Isto pode ser necessário em cenários onde a quantidade de informação processada pela ferramenta torna-se muito grande, obrigando a que a partilha dos mesmos recursos do sistema operativo não seja mais possível. Ou de forma a garantir a redundância da monitorização para o caso de um dos servidores de monitorização falhar o outro poder continuando a fornecer as informações de monitorização.

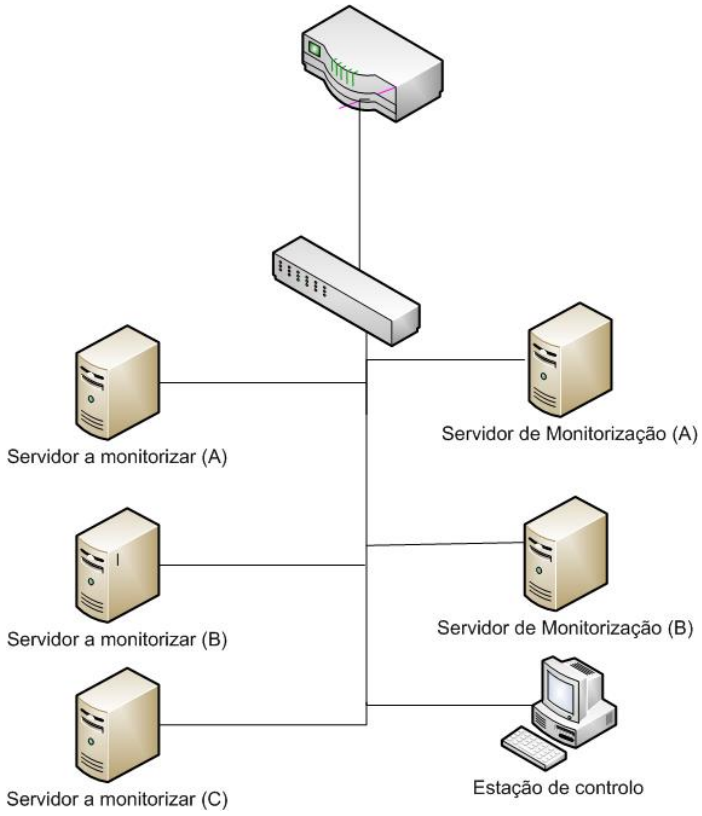


Figura 4.2 – Uso de dois servidores de monitorização
Fonte: Autor

4.2.2 Preparação do servidor de monitorização

O Nagios é uma ferramenta que foi desenhada primeiramente para o sistema operativo Linux, mas pode também ser executado em outros sistemas *Unix*.

O sistema operativo adoptado pelo Sector de Informática do ISUTC para a gestão dos seus servidores é a distribuição de Linux: *Ubuntu 8.04 LTS Server Edition*. Sendo assim, esse será o sistema operativo a usar para preparar o servidor.

Durante a instalação do Nagios foi configurada a interface gráfica com conjunto mínimo de *plugins* para que este tenha alguma funcionalidade, neste caso, as pretendidas para a realização deste projecto. Para este efeito são feitos, anteriormente, *downloads* tanto do Nagios como dos *plugins* do site oficial.

Começou-se pela instalação do Nagios no servidor com o sistema operativo já instalado. Para a instalação do Nagios foi utilizado o manual "*Quickstart Installation Guide*"[S10] presente na sua documentação. Isto consistiu na instalação da aplicação, activação do servidor Apache, para que seja feita a monitorização em ambiente gráfico, e instalação dos *plugins*. Após tudo isso, procedeu-se à aprendizagem da monitorização de computadores com sistema operativos Linux/Unix, Windows, e serviços de acesso público, como o *HTTP*, *FTP*, *SSH*, entre outros. Com isto, manusear os ficheiros de configuração do Nagios, verificar a sua integridade e reactivar o Nagios após alterações na configuração, tornaram-se hábitos que atribuíram ao autor uma muito maior familiaridade com esses mesmos ficheiros.

A estrutura do sistema de ficheiros onde o Nagios é instalado pode ser vista na figura 4.3:

Figura 4.3 – Sistema de ficheiros no directorio raíz do nagios
Fonte: Autor

Na pasta *bin*, encontra-se o próprio Nagios, ou seja, o executável pertencente à aplicação. Encontra-se também outra aplicação Nagiostats, que apresenta estatísticas em relação à execução do Nagios, permitindo posteriormente que se optimize o desempenho do próprio. A seguir tem-se a pasta *etc* onde se encontram todos os ficheiros de configuração pertencentes ao Nagios. Nestes são, por exemplo, indicados os *SLAs* com os quais a aplicação deverá funcionar, bem como são definidos *hosts* e serviços. A alteração de uma qualquer configuração não terá qualquer efeito sobre a aplicação enquanto não se reiniciar o Nagios. Porém, por segurança deverá ser sempre feita a verificação dos ficheiros de configuração para

que se tenha a certeza de que as alterações à configuração respeitam a estrutura destes ficheiros:
/usr/local/nagios/bin nagios -v /usr/local/nagios/etc/nagios.cfg

Após essa verificação, dever-se-á dar procedimento ao reinicio do Nagios:
/etc/init.d/nagios restart

O Nagios, ao contrário da maioria das ferramentas de monitorização, não contém quaisquer mecanismos internos para verificação de estado de serviços que se desejem monitorar. Ao invés disso, acrescenta uma camada de abstracção, os *plugins*, que consistem em executáveis compilados, ou *scripts*, que são livres de verificar o estado de um qualquer serviço, retornando depois um valor cujo formato é estipulado como um protocolo de comunicação entre os *plugins* e o próprio Nagios, definido na documentação. Estes *plugins* encontram-se na pasta *libexec*. Em relação às restantes pastas, são as menos utilizadas, onde no *sbin* se armazenam os ficheiros *cgi* que permitem a parametrização remota do Nagios através da interface *Web*, a pasta *share* onde se encontram as páginas *Web* da já referida interface, e a pasta *var* onde estão os ficheiros de *log*.

A recolha, de parâmetros aplicacionais e do sistema, é feita pelos *plugins*, situados na pasta *libexec*, de onde se realçam os seguintes:

Plugins	Descrição
check_load	percentagem de *CPU* em utilização
check_swap	percentagem de memória swap utilizada
check_procs	número de processos em execução no sistema
check_disk	percentagem do disco utilizado
check_file_age	tempo de vida de ficheiros
check_users	número de utilizadores activos no sistema
check_dhcp	verifica a disponibilidade do servidor *DHCP*
Plugins	Descrição
check_dns	verifica a disponibilidade do servidor *DNS*
check_disk_smb	verifica a disponibilidade do servidor *SAMBA*
check_ftp	verifica a disponibilidade do servidor *FTP*

check_http	verifica a disponibilidade do servidor *HTTP*
check_ldap	verifica a disponibilidade do servidor *LDAP* (autenticação)
check_nagios	verifica o estado do Nagios local ou remotamente (útil em cenários distribuídos)
check_oracle	verifica a disponibilidade do servidor de base de dados *Oracle*
check_ping	verifica o acesso da rede a um dispositivo remoto
check_ smtp	verifica a disponibilidade do servidor *SMTP*
check_pop	verifica a disponibilidade do servidor *POP*
check_ssh	verifica o acesso via *SSH* a terminais remotos
check_snmp	verifica o estado de dispositivos através do protocolo *SNMP*

Tabela 4.2 - Lista dos plugins principais
Fonte: Autor

A definição de *Service Level Availability (SLAs)* é feita nos ficheiros de configuração. Essa informação é definida como parâmetros, na definição dos serviços, a serem enviados, aos comandos sobre a forma de *Macros*. Pode-se tomar como exemplo o caso da verificação da quantidade de disco utilizada:

/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /

Neste caso está-se a especificar que se a partição de disco, onde está montada (comando *mount*) a directoria *root* (raiz) "/", tiver mais de 20% de espaço livre, o estado retornado é "*OK*"; se tiver menos de 20% de espaço livre e mais de 10%, o estado retorna é o de "*WARNING*"; se tiver menos de 10%, o estado retornado é o de "*CRITICAL*".

Verificações de estado

Quanto aos tipos de verificações de estado de serviços ou de terminais, existem dois: activo e passivo. Nas verificações activas, da qual fazem parte as indirectas, o Nagios, é quem inicia a verificação, enquanto que nas verificações passivas, a verificação é iniciada por um processo externo. Isto é particularmente útil, no caso de verificações de serviços assíncronos, como é o caso dos *SNMP traps*, e nos casos em que os serviços encontram-se por detrás de *firewalls*, cuja rede não se tem acesso, mas que permite o acesso das máquinas monitorizadas ao monitor.

Alarmes e notificações

Em relação aos alarmes, estes são feitos através de notificações. Estas consistem no alerta a um, ou conjunto de, contactos associados a um serviço ou a um *host*. As notificações podem ser feitas de qualquer forma, desde um simples *mail*, a um *sms*. Porém, antes dos contactos associados serem notificados, há que filtrar essas mesmas notificações. Isto permite maior flexibilidade no controlo da notificação pois, apesar destas serem sempre lançadas na ocorrência de problemas, nem sempre se desejam notificar os contactos, por exemplo, em horários pré-estabelecidos onde se sabe que um determinado servidor encontra-se desligado para manutenção ou actualização. O Nagios também permite uma definição extremamente flexível no que diz respeito a períodos de tempo em que se se deve notificar um contacto, desde a exclusão de notificação nos dias de férias, alterando neste caso o contacto para outro administrador, até à especificação das semanas alternadas em que alguém, alternadamente com outro contacto, é quem deve ser notificado.

Redundância

Outra grande funcionalidade, do Nagios, consiste na monitorização redundante e à prova de falhas. A ideia básica é a de se terem dois terminais de monitorização: *master* e *slave*, onde este último nada faz enquanto o primeiro funciona. Num cenário mais simplista, pode-se facilmente implementar isto fazendo com que o *slave* monitorize todos os serviços que o *master* monitora, mas com notificações desactivadas, dando a ilusão de nada estar a fazer, enquanto que simultaneamente monitora o *master* através de um serviço que execute o comando *check_nagios* e que esteja associado a um *event handler*. Caso este falhe, com o auxílio dos *event handlers*, apenas terá de activar as notificações nele próprio, ou seja, no *slave*. Contudo, esta abordagem apesar de funcional, não é apropriada a redes de maiores proporções, visto que vários monitores estariam a monitorar os mesmos serviços simultaneamente, consumindo largura de banda à rede. Isto pode-se facilmente resolver com a desactivação das notificações e verificações de estado de serviços, com a activação da recepção de comandos externos, e com a execução duma aplicação externa (*cron*) que periodicamente verifique o estado no *slave* (*check_nrpe*) do *master* (*check_nagios*) inserindo, consoante o valor de retorno, um comando na configuração *external command file* especificado no ficheiro de configuração principal. Este comando teria como função activar ambas as notificações e as verificações dos serviços. Assim, fica-se apenas com um último problema, que é o do *slave* não ter estado inicial de tudo aquilo que monitora. Isto, por sua

vez, resolve-se com a ajuda do *addon NSCA* que permite ao *master* comunicar directamente ao *slave* o estado de tudo o que monitorizam.

Outras funcionalidades

O Nagios também permite a detecção de serviços intermitentes, ou *flap detection*. Isto é feito estudando a variação de estado do serviço nas últimas verificações feitas e, caso a percentagem de alternâncias seja maior que um valor pré-definido nos ficheiros de configuração, são notificados os respectivos contactos desse estado.

Outro aspecto importante consiste na marcação de *downtimes* para serviços que se desejem actualizar ou alterar. O Nagios contém três tipos: fixos, flexíveis e disparados Os fixos começam e terminam nos tempos especificados. Os flexíveis não têm tempos de início nem de fim, apenas a duração. Isto é útil quando sabe-se que um determinado serviço vai-se encontrar em baixo mas não se sabe exactamente quando. Os disparados são activados por um outro evento, tipicamente a falha de outro terminal ou serviço especificado. Isto é extremamente útil em casos de *downtimes* em massa.

O estado das verificações feitas no Nagios não depende única e exclusivamente do estado do serviço monitorizado. Opcionalmente, pode-se fazer uma verificação depender de outra ou outras. A isto se chama *dependency checks*. Isto permite monitorar o estado de serviços remotos com base no estado de outros, permitindo assim melhor correlação dos resultados obtidos entre várias verificações.

Configurações

Quanto às configurações no ficheiro de configuração principal e nos restantes, é importante que sejam tomadas medidas para prevenir o abuso de recursos, fornecidos pelo Nagios, por parte de terceiros. Consequentemente, não se deve executar o Nagios com o utilizador *root* por exemplo, pois este não necessita de permissões do *root* para se executar, e nunca se deve dar a uma aplicação mais permissões do que as de que necessita. Caso seja necessária a execução de aplicações ou *scripts* por parte de, por exemplo, *event handlers* é aconselhável a utilização do comando *sudo*. É igualmente importante verificar as permissões de leitura e escrita do directório indicado, no ficheiro principal de configuração, como o *check_result_path*. Nesta são colocadas as respostas recebidas, resultantes das verificações feitas, antes de serem processadas. Acessos indevidos a esta pasta poderão resultar na falsificação de verificações, ou na sua eliminação. Outro aspecto, também a nível de

segurança, é o controlo de acessos ao ficheiro de comandos externos, caso esta funcionalidade esteja activada em *check_external_commands*. O acesso só deverá ser permitido ao utilizador do Nagios, tipicamente *nagiosuser*, e ao utilizador com o qual é executado o servidor *Web*, tipicamente *nobody* ou *httpd*.

Outra forma de controlar o Nagios é através de *CGIs*, normalmente inserindo-se comandos externos no ficheiro de comandos externos, pelo que é aconselhável que se faça autenticação antes de se ter acesso a esses *CGIs*. Esses mesmos *CGIs* têm acesso, tanto ao ficheiro principal de configuração, como às restantes configurações na pasta *etc* (figura 4.3). Por essa razão, não se devem armazenar *usernames* e *passwords* nesses ficheiros. O correcto é utilizar macros *$USERn$* que são definidos no ficheiro */etc/resource.cfg*. O Nagios dá a garantia de que os *CGIs* não tentarão ler desse ficheiro, pelo que pode-se restringir o acesso a este dando-lhe permissões *600* ou *660*, ou seja, de leitura apenas ao dono e aos utilizadores pertencentes ao mesmo grupo do dono.

Apresentação de Dados

A apresentação de dados resultantes da monitorização é feita através de um *browser*. Tem-se facilmente acesso aos dados que são gerados numa página *Web* através do *URL http://ip.do.servidor/nagios*. Ao aceder a esta página, será requisitado ao utilizador um *username* e uma *password*. A página encontra-se dividida em vistas:

Teste prático

O seguinte teste prático, demonstrado na figura 4.4 visa focar os seguintes aspectos:

- Monitorização de parâmetros de sistema – Anexo 2;
- Monitorização de servidores *HTTP, IMAP, POP3, SMTP, SSH, PING* e *DNS*;

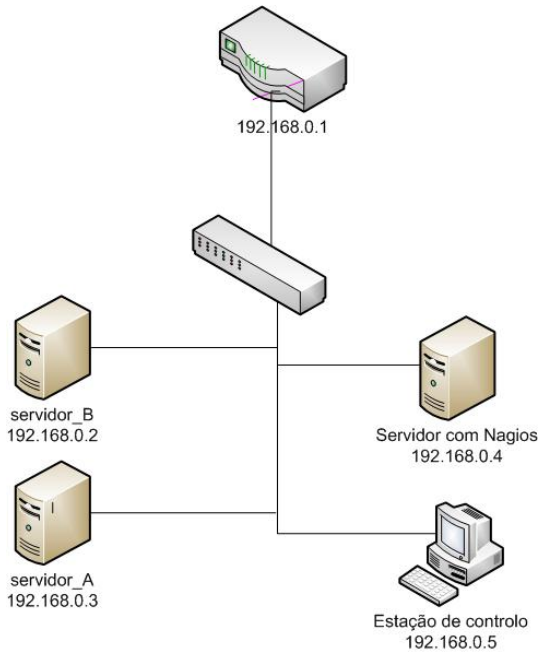


Figura 4.4 – Cenário de teste
Fonte: Autor

A estação de monitorização (192.168.0.4) procederá à monitorização do servidor_A (*FTP*, *PING*, *SSH*) – Anexo 2; e do servidor_B (*HTTP*, *IMAP*, *PING*, *POP3*, *SMTP* e *DNS*) – Anexo 3. Para se montar este cenário de testes foi necessário fazer configurações no servidor de monitorização – Anexo 4 e 5.

Ferramentas adicionais

De modo a poder instalar o Nagios, foi necessário instalar as seguintes ferramentas adicionais:

- *postfix* – é um servidor para envio e entrega de *e-mails*.
- *mailx* – é um programa cliente utilizado para envio e leitura de e-mails.

4.3 Apresentação de resultados

Após efectuar os testes com o sistema de monitorização foi possível obter os seguintes resultados:

- O sistema permitiu verificar a disponibilidade dos servidores;
- O sistema permitiu verificar a disponibilidade de cada serviço de rede instalado em cada servidor;

- O sistema enviou notificações de falha dos serviços ao administrador da rede através do seu contacto de e-mail;
- O sistema permitiu gerar relatórios dos eventos ocorridos;
- O sistema apresenta uma interface de administração amigável e fácil de administrar;
- A carga de memória resultante do uso do sistema no servidor é reduzida.

4.4 Orçamento do Projecto

Item	*Qtd.*	*Preço unitário (MT)*	*Preço total (MT)*
Intel Core 2 Duo, 2 GHZ, 2 GB RAM, 250 GB HDD, Monitor 19", Teclado e Mouse	1	28.750,00	28.750,00
Preparação do servidor	-	10.000,00	10.000,00
Instalação do Nagios	-	17.500,00	17.500,00
Formação (6 horas)	-	10.000,00	10.000,00
Total			66.250,00

Tabela 4.3 - Orçamento do projecto
Fonte: Autor

A manutenção do servidor não consta do orçamento pois ficará a cargo dos administradores de rede do ISUTC.

Após a implementação do sistema em causa é gerado um retorno imediato expresso na possibilidade de os administradores de rede poderem fazer um acompanhamento dos servidores e serviços em operação e podendo agir prontamente em caso de se registar uma falha, uma vez que o sistema envia notificações sobre os estados de operação.

CAPÍTULO 5 CONCLUSÕES E RECOMENDACÕES

5.1 Conclusões

Um dos grandes objectivos deste trabalho foi a implementação de um sistema de monitorização na rede de computadores do ISUTC e considera-se com sucesso. Depois da realização deste trabalho foram retiradas as seguintes conclusões:

- Foram identificados os serviços de rede implementados na rede do ISUTC, sendo que era de grande importância que estes fossem identificados de modo a melhor determinar como será o funcionamento do sistema implementado. Existindo uma variedade de serviços notou-se que é vital que se garanta que todos os serviços estejam sendo monitorizados continuamente pois se um deles falhar, o tempo de identificação do problema tem que ser o menor possível de modo a que se possa responder rapidamente ao problema.
- Foram identificados os problemas rede existentes e também os mais frequentes, pois é com base nestes que o estudo se baseia. A maioria dos problemas que surgem afectam de forma significativa não só o desempenho da rede, mas também os utilizadores que dependem dos serviços para poderem realizar as suas actividades e tarefas.
- Foram definidos os sistemas de monitorização existentes, mediante uma pesquisa bibliográfica exaustiva em alguns livros e páginas da Internet. Existem vários sistemas de monitorização que por sua vez possuem vantagens e desvantagens, cabendo então ao administrador de rede saber equilibrar a avaliação dos sistemas de forma a fazer a escolha do que melhor pode responder aos problemas.
- Após a avaliação dos sistemas existentes, foi escolhido um sistema com base nos requisitos funcionais que cada um apresentava, e que veio a ser implementado e tendo-se efectuado testes utilizando-o. Tendo uma implementação do sistema foi possível obter resultados que responderam as necessidades dos administradores da rede.

5.2 Recomendações

Após a realização deste trabalho foram elaboradas as seguintes recomendações:

- Enquadrar o sistema implementado nas políticas de segurança adoptadas pelo ISUTC no que diz respeito a rede de computadores;
- Elaborar um manual de procedimento de quem e quando deve aceder o sistema de forma a se atingir o propósito principal do seu uso;
- Estudar possível implementação do sistema num servidor utilizando a virtualização;
- Identificar fragilidades do sistema de forma a melhorá-lo;
- Identificar outros tipos de sistema de monitorização de forma a garantir a estabilidade da rede (por exemplo de tráfego);
- Integrar o Nagios com o servidor de e-mail local (Zimbra).

Recomendações para trabalhos de investigação futuros:

- Integrar outro módulo de autenticação de utilizador do Nagios;
- Implementação de sistemas de monitorização de redes remotas;

REFERÊNCIAS BIBLIOGRÁFICAS

Livros

[L1] Tanenbaum, A. S. (2003). Redes de computadores. 4ª edição, Editora Campus.

[L2] Junior, E. I. (2003). *Uma Proposta de Metodologia para Análise de Desempenho de Redes IEEE 802.11 Combinado a Gerência SNMP e Ferramentas de Simulação.* Tese de Mestrado, Instituto Nacional de Telecomunicações.

Sites

[S1] Pinheiro, J. M. S. Gerenciamento de Redes de Computadores: Uma Breve Introdução.http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php.

[S2] Oliveira, T. S. Gerenciamento de redes TCP/IP. http://www.webartigos.com/articles/19661/1/Gerenciamento-de-Redes-TCPIP/pagina1.html.

[S3] Introdução a Gerenciamento de Redes TCP/IP. http://www.rnp.br/newsgen/9708/n3-2.html.

[S4] Gerenciamento de Redes TCP/IP – continuação. http://www.rnp.br/newsgen/9712/gerencia.html.

[S5] M.3000 : Overview of TMN Recommendations. http://www.itu.int/rec/T-REC-M.3000-200002-I/en.

[S6] FCAPS. http://www.worldlingo.com/ma/enwiki/pt/FCAPS.

[S7] Router. http://www.webopedia.com/TERM/R/router.html.

[S8] Switch.http://compnetworking.about.com/od/hardwarenetworkgear/g/bldef_switch.htm.

[S9] O Gerenciamento de redes. http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/gerenciamento/.

[S10] Nagios. http://www.nagios.org

[S11] OpenNMS. http://www.opennms.org

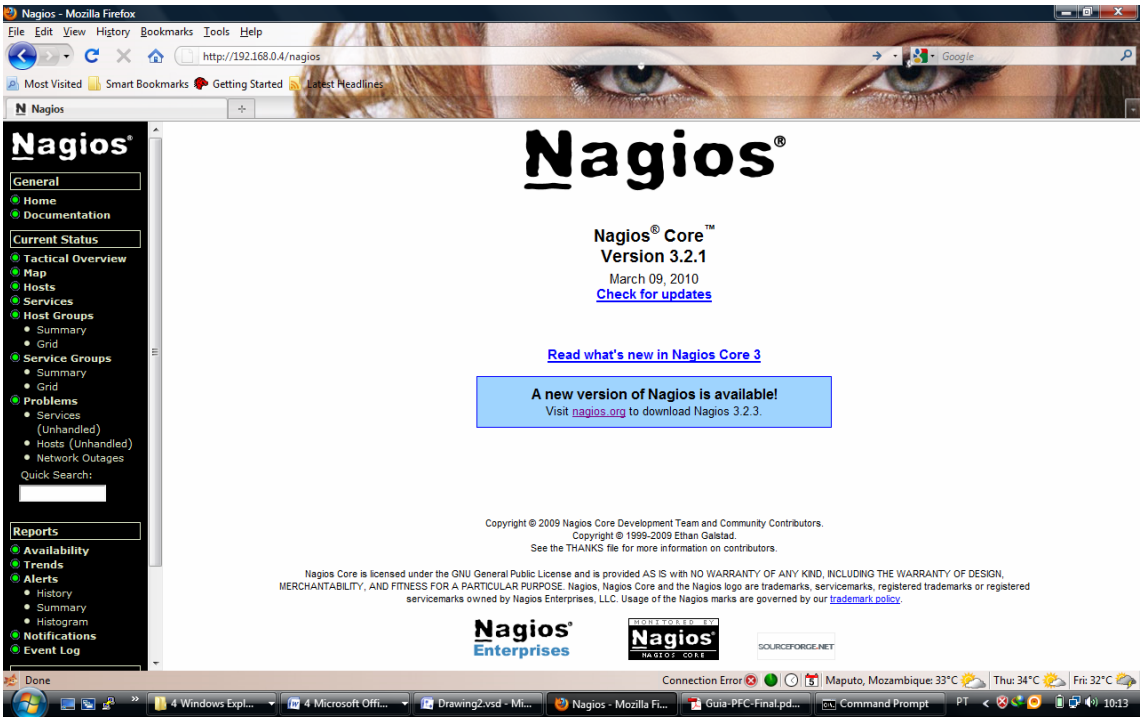
[S12] Cacti. http://www.cacti.net

BIBLIOGRAFIA

- Parker, T. e Siyan K. S. (2002). TCP/IP UNLEASHED. 3ª edição, Editora Sams. Indianapolis.
- Loureiro, P. (2003). TCP/IP em Redes Microsoft. 6ª edição, FCA. Lisboa.
- Gerenciamento de rede TCP-IP – continuação. http://www.rnp.br/newsgen/9712/gerencia.html
- Gerenciamento de redes. http://www.gta.ufrj.br/~alexszt/ger/snmpcmip.html

ANEXOS

Anexo 1 – Página inicial do Nagios



Anexo 2 – Monitorização do servidor_A

servidor_A	Current Load	OK	11-04-2010 10:23:19	0d 0h 6m 7s	1/4	OK - load average: 0.35, 0.42, 0.37
	Current Users	OK	11-04-2010 10:19:51	0d 0h 4m 35s	1/4	USERS OK - 1 users currently logged in
	FTP	OK	11-04-2010 10:20:29	0d 0h 3m 57s	1/3	FTP OK - 0.001 second response time on port 21 [220 (vsFTPd 2.0.6)]
	PING	OK	11-04-2010 10:21:07	0d 0h 3m 19s	1/4	PING OK - Packet loss = 0%, RTA = 0.14 ms
	Root Partition	OK	11-04-2010 10:21:45	0d 0h 2m 41s	1/4	DISK OK - free space: / 1188328 MB (88% inode=99%):
	SSH	OK	11-04-2010 10:22:24	0d 0h 2m 2s	1/4	SSH OK - OpenSSH_4.7p1 Debian-8ubuntu1.2 (protocol 2.0)
	Swap Usage	OK	11-04-2010 10:23:02	0d 0h 1m 24s	1/4	SWAP OK - 100% free (9632 MB out of 9632 MB)
	Total Processes	OK	11-04-2010 10:23:02	0d 0h 6m 24s	1/4	PROCS OK: 93 processes with STATE = RSZDT

Anexo 3 – Monitorização do servidor B

servidor_B	Current Load	OK	11-04-2010 10:23:40	0d 0h 5m 46s	1/4	OK - load average: 0.47, 0.44, 0.38
	Current Users	OK	11-04-2010 10:19:19	0d 0h 5m 7s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	11-04-2010 10:19:57	0d 0h 4m 29s	1/4	HTTP OK: HTTP/1.1 200 OK - 13738 bytes in 0.046 second response time
	IMAP	OK	11-04-2010 10:20:35	0d 0h 3m 51s	1/3	IMAP OK - 0.001 second response time on port 143 [* OK zambeze.isutc.transcom.co.mz Zimbra IMAP4rev1 service ready]
	PING	OK	11-04-2010 10:21:14	0d 0h 3m 12s	1/4	PING OK - Packet loss = 0%, RTA = 0.02 ms
	POP3	OK	11-04-2010 10:21:52	0d 0h 2m 34s	1/3	POP OK - 0.001 second response time on port 110 [+OK zambeze.isutc.transcom.co.mz Zimbra POP3 server ready]
	Root Partition	OK	11-04-2010 10:22:30	0d 0h 1m 56s	1/4	DISK OK - free space: / 1188323 MB (88% inode=99%):
	SMTP	OK	11-04-2010 10:23:08	0d 0h 1m 18s	1/3	SMTP OK - 0.001 sec. response time
	SSH	OK	11-04-2010 10:23:09	0d 0h 6m 17s	1/4	SSH OK - OpenSSH_4.7p1 Debian-8ubuntu1.2 (protocol 2.0)
	Swap Usage	OK	11-04-2010 10:23:47	0d 0h 5m 39s	1/4	SWAP OK - 100% free (9632 MB out of 9632 MB)
	Total Processes	OK	11-04-2010 10:19:25	0d 0h 5m 1s	1/4	PROCS OK: 73 processes with STATE = RSZDT

Anexo 4 – Configuração para monitorização do servidor_A

```
define host{
        use                     linux-server
        host_name               servidor_A
        alias                   servidor_A
        address                 192.168.0.3
        }
define service{
        use                     local-service
        host_name               servidor_A
        service_description     PING
        check_command           check_ping!100.0,20%!500.0,60%
        }
define service{
        use                     local-service
        host_name               servidor_A
        service_description     Root Partition
        check_command           check_local_disk!20%!10%!/
        }
define service{
        use                     local-service
        host_name               servidor_A
        service_description     Current Users
        check_command           check_local_users!20!50
        }
define service{
        use                     local-service
        host_name               servidor_A
        service_description     Total Processes
        check_command           check_local_procs!250!400!RSZDT
        }
define service{
        use                     local-service
        host_name               servidor_A
        service_description     Current Load
        check_command           check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
        }
define service{
        use                     local-service
        host_name               servidor_A
        service_description     Swap Usage
        check_command           check_local_swap!20!10
        }
```

```
define service{
        use                     local-service
        host_name               servidor_A
        service_description     SSH
        check_command           check_ssh
        notifications_enabled   0
        }
define service{
        use                     generic-service
        host_name               servidor_A
        service_description     FTP
        check_command           check_ftp

        }
```

Anexo 5 – Configuração para monitorização do servidor_B

```
define host{
        use                     linux-server
        host_name               servidor_B
        alias                   servidor_B
        address                 192.168.0.2
        }
define service{
        use                     local-service
        host_name               servidor_B
        service_description     PING
        check_command           check_ping!100.0,20%!500.0,60%
        }
define service{
        use                     local-service
        host_name               servidor_B
        service_description     Root Partition
        check_command           check_local_disk!20%!10%!/
        }
define service{
        use                     local-service
        host_name               servidor_B
        service_description     Current Users
        check_command           check_local_users!20!50
        }
define service{
        use                     local-service
        host_name               servidor_B
        service_description     Total Processes
        check_command           check_local_procs!250!400!RSZDT
        }
define service{
        use                     local-service
        host_name               servidor_B
        service_description     Current Load
        check_command           check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
        }
define service{
        use                     local-service
        host_name               servidor_B
        service_description     Swap Usage
        check_command           check_local_swap!20!10
        }
```

```
define service{
        use                     local-service
        host_name               servidor_B
        service_description     SSH
        check_command           check_ssh
        notifications_enabled 0
        }
define service{
        use                     local-service
        host_name               servidor_B
        service_description     HTTP
        check_command           check_http
        notifications_enabled 0
        }
define service{
        use                    generic-service
        host_name               servidor_B
        service_description     SMTP
        check_command           check_smtp
        }
define service{
        use                     generic-service
        host_name               servidor_B
        service_description     POP3
        check_command           check_pop
        }
define service{
        use                     generic-service
        host_name               servidor_B
        service_description     IMAP
        check_command           check_imap
        }
```