EVENT MONITORING IN A SMALL AND BUSINESS ENTERPRISE

Nuno Quaresma, Mestre em Administração de Redes e Sistemas Informáticos, ISPGaya[1]

Vasco Miranda, Docente do ISPGaya[2]

Fernando Almeida, Docente do ISPGaya[3]

António Baixinha, Responsável pelo Serviços de Informática da DURIT[4]

Resumo: Este artigo apresenta uma visão geral do papel e responsabilidades de um administrador de sistema, focando-se na necessidade de monitorização da infraestrutura tecnológica. A monitorização da infraestrutura informática é, atualmente sem dúvida, um dos pontos principais de suporte ao negócio. As grandes empresas não são exclusivamente as únicas que sentem necessidade em usar ferramentas de monitorização, mas as pequenas e médias empresas, que também possuem ambientes TI com cada vez maior complexidade, sentem a mesma necessidade. Esta situação tem impacto diretamente nas operações que são suportadas por plataformas TI no apoio às pessoas e processos. Quando um sistema, que é vital para a organização, falha tanto a nível de hardware como software, compromete a capacidade operacional e consequentemente a continuidade do próprio negócio. Tendo isto sempre em mente, torna-se extremamente importante a adoção de sistemas de monitorização que proactivamente ou reactivamente, reduzam o tempo total de avarias causadas por falhas. Um sistema de monitorização é o meio para garantir confiança em todos os componentes e a disponibilidade operacional da infraestrutura TI.

Palavras-chave: Monitorização TI; Redes de Computadores; Administração de Sistemas; Protocolos; Zabbix; SME.

[1] nmcq@ispgaya.pt
[2] vcm@ispgaya.pt
[3] falmeida@ispgaya.pt
[4] antonio.baixinha@grupodurit.pt

EVENT MONITORING IN A SMALL AND BUSINESS ENTERPRISE

Abstract: This paper presents an overview of the role and responsibilities of the system administrator, focusing on the need to monitor its technological infrastructure. The informatics infrastructure monitoring is, nowadays without a doubt, one of the main key points in business support. Large enterprises are no longer the only ones to feel the need to use these monitoring tools, but small and medium-sized enterprises, which also have IT environments of an increasing complexity, feel such a need. This results directly from the operation of how the business is supported on IT platforms as support for people and processes. When a system, which is vital to the organization, fails either at the hardware or software level, compromises the operating capacity and consequently the business continuity. Having this always in mind, it is extremely important to adopt monitoring systems that proactively or reactively, reduce the overall time of breaks caused by failures. A monitoring system is the way to ensure confidence in all components and the operational readiness of IT infrastructure.

Keywords: IT Monitoring; Computer Networks; System Administration; Protocols; Zabbix; SME.

1 INTRODUÇÃO

Small and medium-sized enterprises currently have a more or less complex computing infrastructure, depending on the area of activity and on their needs. As time goes by, the computer networks have been growing and increasingly demands the administration of its infrastructure, starting the need of bring a proactive in the resolution of problems as they emerge.

As a result of this increase in infrastructures, the number of occurrences of problems kept the same direction. In this sense the monitoring infrastructure gained importance (even though often neglected), but increasingly essential in small and medium sized Portuguese companies, which are increasingly more dependent on new technologies in support of its main activity.

This was the main reason for the choice of the theme, the management and monitoring of a network infrastructure asset, opting for open source tools, or free use, making the project less dependent on financial issues that could eventually derail. We only feel the lack of new information and communication technologies when they fail. Infrastructure monitoring aims to reduce the possibility of occurrences that may cause the failure of services, which are essential in everyday life.

This article starts by making a contextualization of the monitoring systems, with State of the art. Then we have the implementation, where the presumed requirements of the solution are described. In point IV, are the main results explained, and the best practices to be taken into consideration in the implementation of a monitoring solution. Last but not least, the conclusions and the description of the work can be done in the future.

2 STATE OF THE ART

2.1 Computer Networks

According to Teixeira (1999) a network is nothing more than a set of interrelated components and systems. Computer networks are becoming increasing complex, even in small and medium-sized enterprises (SMEs). If we initially only had a local area network with some computers connected by a copper wire, today we also have fiber optic connections and wireless Internet, which in itself creates a wider variety of hardware features and associated protocols. Most part of the computer infrastructure currently have multiple servers that are home to more and more services, multiple switches, routers, access points, printers, access control terminals, firewalls, among others, becoming extremely complex in its management and maintenance. In addition

to all this complexity, there are also cloud services and links between various geographically distributed locations, which can be done through Virtual Private Networks (VPN) or MPLS (Multi Protocol Label Switching) (Tanenbaum, 2003).

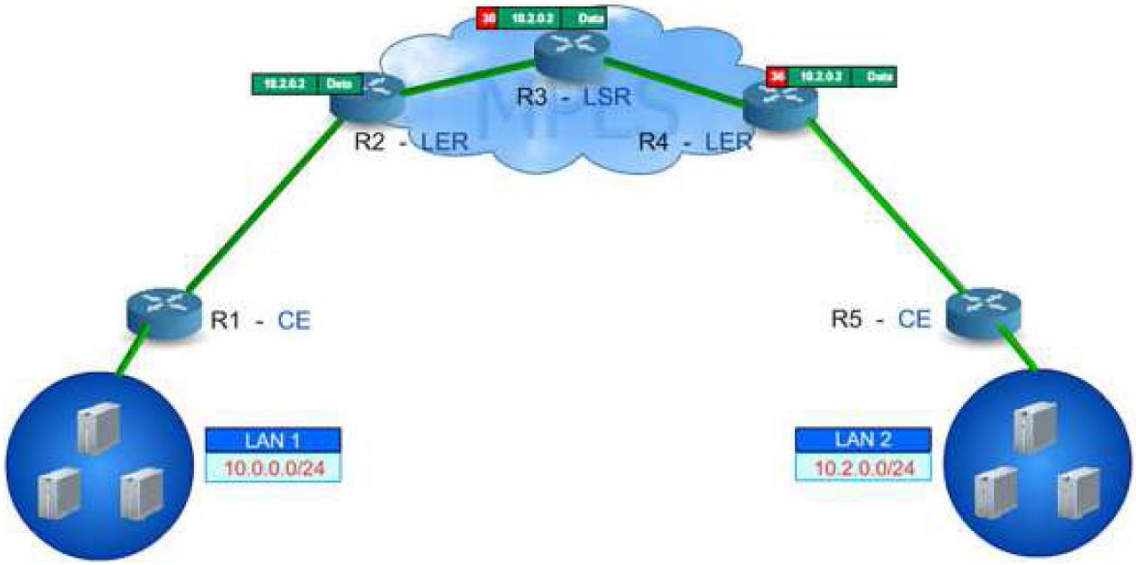

Figure 1: MPLS architecture (Faucheur et al., 2002)

The MPLS architecture allows the user to connect several local networks (Fig. 1), and the level of the OSI model will appear in an intermediate layer to the traditional definitions of Layer 2 (link) and Layer 3 (network) (Fig. 2).

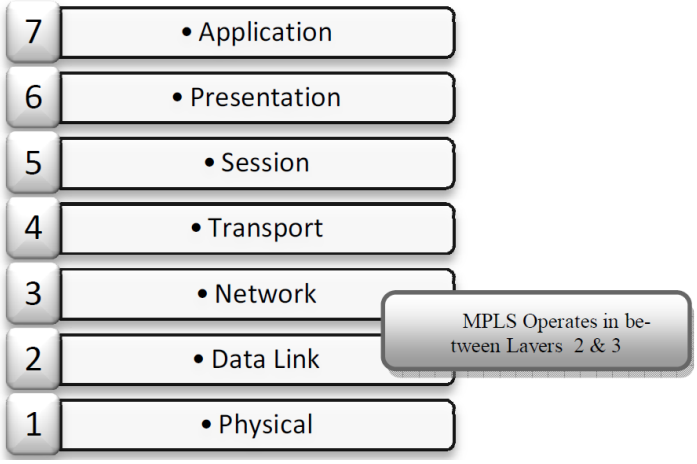

Figure 2: MPLS in the OSI model (MPLSINFO, s.d.)

2.2 Essential Protocols

The successful implementation of a monitoring solution is only possible with the use of Simple Network Management Protocol (SNMP), much of the hardware for example printers, switches, or the gathering of information is made using this protocol (SNMP, s.d.).

SNMP is an application-level protocol that makes the exchange of information easier between the server, where the solution and agents residing in the managed components, such as routers, switches, printers, among others is implemented. An SNMP-managed network has three key elements: managed devices, the agents and the management stations. Through this infrastructure, SNMP provides network administrators information about resource use and alarms, which allows you to identify and solve problems, and plan for network growth. The managed devices collect and store the information in its database (MIB-Management Information Base) and provide it via SNMP, to management stations. The agent has specific function to collect the data stored in the MIB and to turn them into SNMP-compliant information. The model MIB that comprises the database related to traffic data is the MIB-II. The Organization of this model contains a set of groups that monitor the execution of multiple protocols on the network element, such as IP, TCP/UDP, BGP, OSPF, providing the state (active/inactive) of an equipment or accounting statistics of counters of bytes and packets sent, received or lost for each interface. They also offer information about relevant data relating to the performance of the device, such as CPU utilization and memory.

2.3 Monitoring Tools

For the vision of the European Union on a European Research Area (ERA), was drafted a manual of good practice entitled "*monitoring tools for Network Services and systems*" by GÉANT. This manual provides a list of monitoring solutions that will be the basis of study of this project. The manual indicates the main characteristics of each of the solutions: Nagios (also Icinga), Munin, ManageEngine OpManager, ManageEngine DeviceExpert, MetaNav, Netdisco, Smokeping, What's UP, Zabbix, Zino.

Much of the monitoring solutions end up having common characteristics, and this article is going to focus on solutions with low cost of implementation and use.

When monitoring begins to be planned, both the user and the system administrator must have a clear idea of what should be monitored. There are many, but not all services can be monitored, with the risk of having excessive and unnecessary information. Too much information can also

lead to greater difficulty in tracking the changes. Changes in data-processing Park will always be more difficult to manage and to change the sensors correctly if in reality the system administrator is to monitor services that would not be necessary. The definition of the parameters to be monitored, can avoid a flurry of alarms. The administrator must have his system configured only to receive alerts that effectively will deserve some kind of treatment (NETDISCO, s.d.). When monitoring implementation is being planned, it is important to take into account other perspectives, and make adjustments according to who will use the solution. A team that manages a computer Park does not need to receive all the same information, and if it is sent to the proper recipient, you can limit crashes and reduce redundancy.

All these aspects to be taken into account, will allow better monitoring of the system and an easier adaptation to future changes.

2.4 Licensing Costs

Licensing costs of a solution to monitor a company's computing infrastructure is a fundamental aspect. It is not always easy to raise the awareness of the administration of an enterprise to the need of monitoring the data-processing park. It is the system administrator' task to raise the awareness of the company's administrators of the need to implement a solution so that you can monitor the computer network, but the process is much simpler if you choose free or open source solutions (Silveira, 2003).

The General Public License (GPL) is a license that accompanies the software distributed by the GPL project, and has a wide range, including the core of the Linux operating system. The other alternative is the Open Source Software, which is the software that was delivered with a publicly viewable source code, that is, according to the definition established by the Free Software Foundation is any computer program that can be used, copied, studied, modified and redistributed with some restrictions (FSF, s.d.; SLO, 2008). This model of software is usually developed by communities, where geographically dispersed individuals, share knowledge, using simple tools to coordinate and communicate their work over the Internet (Engelfriet, 2005).

Open Source Software, respects the four freedoms defined by the Free Software Foundation, however, it does not establish certain restrictions such as those contained in the GPL. They are:

- The freedom to run the software, for any purpose (it does not have restrictions on the part of the supplier);

- The freedom to study how the program works, and adapt it to your needs. Access to the source code is a prerequisite;
- The freedom to redistribute copies;
- The freedom to improve the software, and publish their improvements, so that the whole community can benefit access from the access to the source code.

2.5 Zabbix

ZABBIX, is one of the tools that has been steadily gaining its space in monitoring solutions, framing the characteristics, features and licensing in the vast majority of small and medium-sized enterprises. The software is distributed under the GNU General Public License (GPL) version 2 and can be used in a commercial context, but the collaboration in the development of Zabbix brings additional benefits in terms of some level of support.

Zabbix supports most operating systems: Linux, Solaris, HPUX, AIX, FreeBSD, OpenBSD, NetBSD, Mac OS, Windows, among others. It allows you to monitor simple services (http, pop3, imap, ssh) without the need to use agents, and an agent to be installed normally in serve pain, that can monitor a lot of parameters, with its sensors.

Zabbix adds some important benefits. It is a single solution (all-in-one) that control small to large distributed environments where all historical data, trends and configuration are stored in a database that can be MySQL, PostgreSQL, Oracle, IBM DB2 or SQLite. Zabbix is also extremely flexible. It allows dealing with unstable communications and offers the possibility of an automatic detection of hardware. The platform enables sending alerts via email, SMS, and custom scripts, and creates real-time graphics regarding the performance and usage level of IT infrastructure. Finally, the web interface and standard SQL databases ensure integration with legacy software.

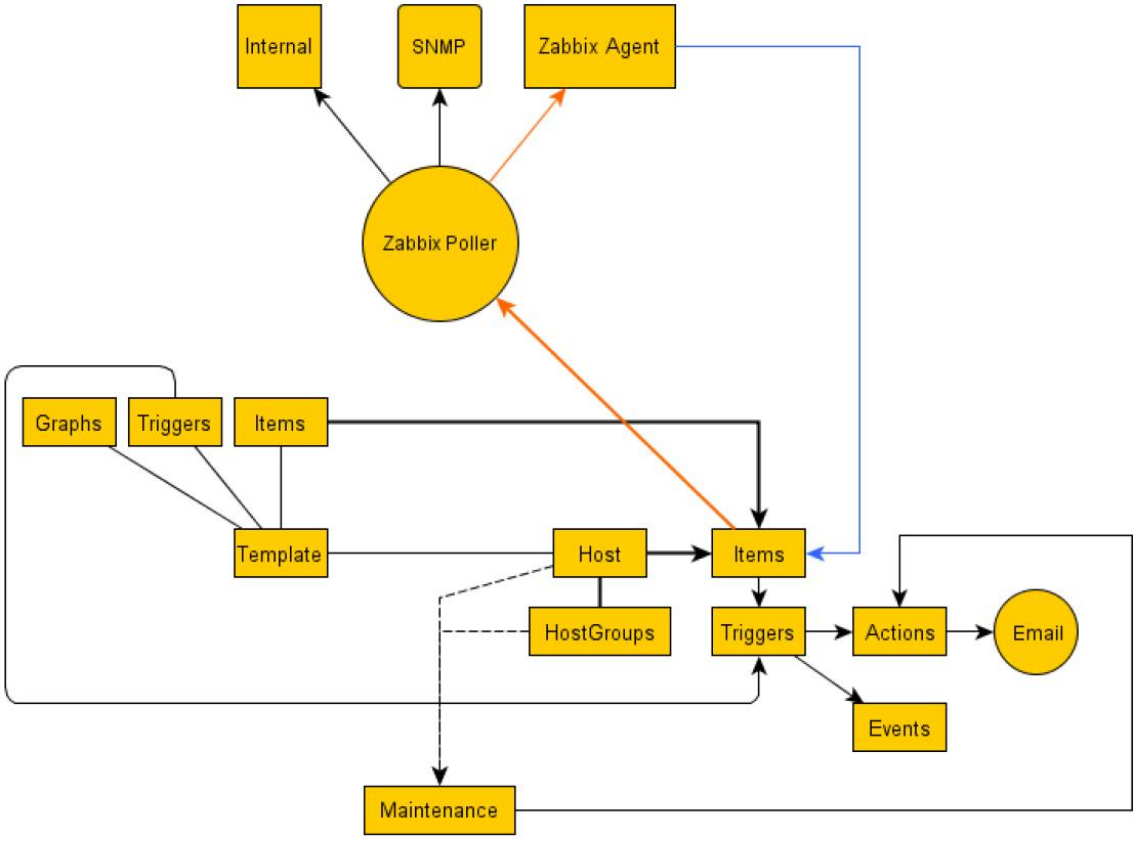

Figure 3: Zabbix architecture (Marcel, 2010)

Zabbix is perfectly structured, in order to help the system administrator (Fig. 3). The use of templates allows the definition of a rules model of collection, alert levels and graphical representations that can be easily applied to monitored elements. Zabbix, has created some templates by default, which are a great base to work with. They allow you to group similar machines so that the criteria for monitoring and alerts being similar, according to the characteristics of the machines. Figure 3 shows the main parameters that are part of a template: Items, Graphs and Triggers.

An item is a single performance parameter or availability; it is a measurable value. To a host is several items associated, according to its characteristics. The graphs allow a better visualization of results and can be configured according to the pretended sensors which can easily be changed at any time. The graphs are configured by the administrator of the solution and can be created to be simple or more complex, according to the information that you want. Finally, the triggers are defined as logical expressions, which represent the State of the system. The triggers are defined in templates, and when they assume a certain logical value, trigger an action or an event, and in the vast majority of cases actions are configured, usually with the alerts that can be sent

by email or SMS. Additionally, host groups allow you to group hosts; the use of host groups is not mandatory, but it helps in the internal organization of information.

Zabbix allows monitoring a quantity and variety of hosts. It supports a wide variety of protocols, Hardware platforms and Operating Systems, this simplifies the implementation, since it will be possible to monitor the infrastructure by grouping hosts according to similar characteristics (Fig. 4).

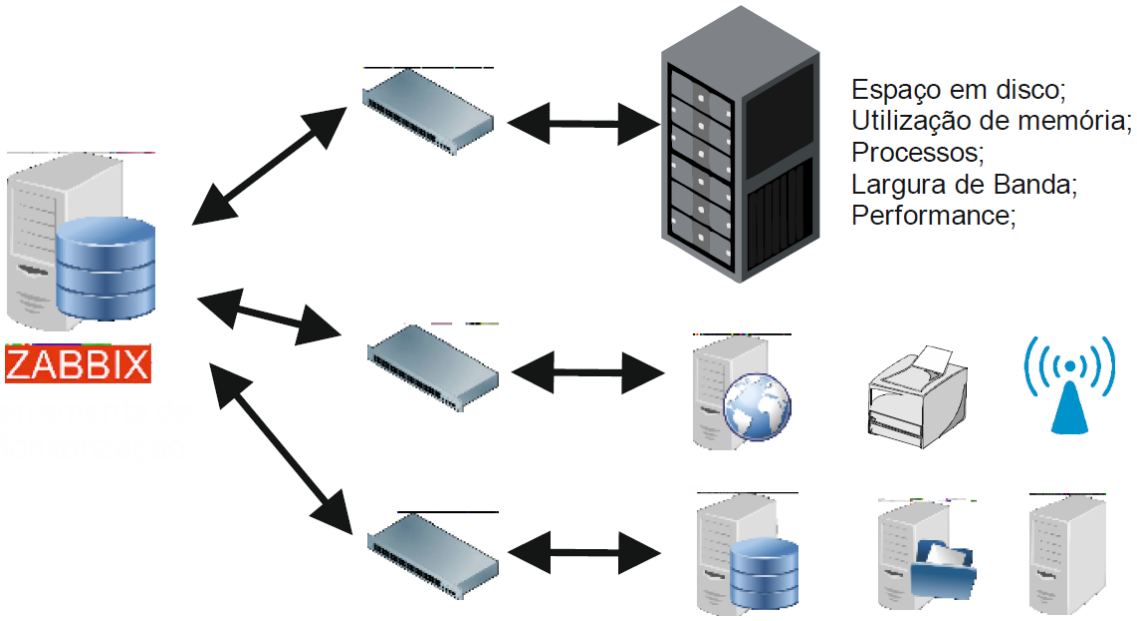

Figure 4: Monitoring of hosts with Zabbix (Zabbix, s.d.)

Zabbix reacts to events by executing a set of operations that is defined as an action. An action is defined for any event or set of events created by Zabbix. Its attributes are: Name, Event source, Enable escalations, Period, Default subject, Default message, Recovery message, Recovery subject, Recovery message and Status (Olups, 2010).

3 APPROACH AND REQUIREMNTS

3.1 Functional Requirements

There are functional requirements that must be taken into account when we choose an IT infrastructure monitoring. Implementing a monitoring solution must allow network and systems administrators to acknowledge clearly what is happening in that infrastructure that they manage. The solution must tend to improve the capabilities in order to be able to react faster and properly to a possible problem. On the other hand, as the infrastructure grows and increases the number of connected systems, it also increases the probability of problematic events, which

you want to decrease by constant monitoring and by using a system that sends alerts to administrators via email.

An appropriate monitoring tool should be used, not only to allow appropriate reactions to problems that may occur, but also to be used as an instrument of preventive policies. For a correct planning of the implementation, it is necessary to draw up a table with a summary of assets, which services it supports, its criticality, monitoring metrics, the criteria for triggering actions and which actions to carry out.

3.2 Non-functional Requirements

For the non-functional requirements, it is important to choose a solution where the implementation is of simple usability with an attractive interface and not depending on specific knowledge by the user. It is important that the implementation does not have implications for infrastructure, being as transparent as possible to other services and users. The solution must be highly available and always easily accessible for users.

The many existing monitoring solutions allow you to make free software implementations and this is always a factor to be taken into account. A monitoring solution must be secure in order to ensure that it is not allowed access to the system by unauthorized users. For a good management it is important that is accessible remotely, so that problems in infrastructure can be quickly detected. Access through a web interface, regardless of the browser used, is another important aspect that the monitoring solution should take into account (NAV, s.d.). It is not only for the solution that will monitor the system must take into account the cost containment, operating system where it will be installed must be based on Open Source and preferably a ' Long Term Support ' for example the Linux Ubuntu Server LTS. It should be based on MySQL databases. The system should be based on the Apache web server, since the vast majority of Open Source implementations use the PHP programming language. Any implementation should be properly documented to facilitate subsequent amendments to implementation (MUNIN, s.d.).

4 DISCUSSION AND GOOD PRACTICES

The successful implementation of a brief monitoring solution depends on the results obtained. Getting results in real time is essential for a good IT infrastructure monitoring.

There is a set of good practices that are essential to ensure that the implementation is successful. The dialogue with administrators of the companies is essential to set the appropriate ITIL rules of organization; after all, they are the ones who have the responsibility of defining the degree of criticality of the given service.

It is important to monitor service levels. Its information on service levels is stored in DB, a solution as Zabbix has information about the uptime of certain service is of extreme importance to the administrator computer Park, but no less important is the quality of service. It is not enough for anyone who manages a computer infrastructure of a company to know that a particular host is connected, it is also essential to know if it is working correctly. One of the key points is to have information on the use of host processor and memory. That particular host having 100% uptime, does not mean necessarily that it is providing its services in an appropriate manner, it is important to have information about the quality of service. For more effective management of the enterprise infrastructure, it is recommended the adoption of a tool that allows managing tickets. This tool will allow you , in the long term, to have a perception of what the hosts that have generated more problems and trace what has been done and by whom it was done to resolve the incident.

The information gathered will allow, in the future, adjusting the ITIL rules to the infrastructure of the company, constantly adapting to a better use of resources.

5 CONCLUSIONS

There is no reason for the system administrator not having the infrastructure monitored. Depending on the infrastructure and available resources, the implementation of a solution to monitor the network has no shortage of alternatives. They can be more or less complex, whether commercial or open source solutions. It is the responsibility of the system administrator to identify the critical services and to implement a solution that allows administrator to monitor the infrastructure.

A correct management of a data-processing park is only possible with constant monitoring. The system administrator may not, under any circumstances, forget to update the information regarding infrastructure. An out of date database can lead to serious errors in planning and managing a network infrastructure in a company.

New solutions for IT do not cease to arise and monitoring solutions are no exception. A constant review of existing solutions on the market is essential to maintain the infrastructure monitored properly.

The study of ticket management solutions, analysis, implementation, and integration with the monitoring tool Zabbix, will be an important contribution to a better management of data-processing IT Park by the teams of the companies.

References

Engelfriet, A. (2005). *Choosing a software license*. Obtained in 26th of April 2013, from Lus Mentis Law and Technology: http://www.iusmentis.com/computerprograms/licenses/choosing/#Standardlicenses

Faucheur, F., Wu, L., Davari, B., Vaananen, P., Krishnan, R., Cheval, P., & Heinanen, J. (2002). *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*. Obtained in 18th December 2012, from http://www.hjp.at/doc/rfc/rfc3270.html

FSF (s.d.). *Free Software Foundation*. Obtained in 11th of March 2013, from FSF: http://www.fsf.org

Marcel (2010). *Logical structure of Zabbix*. Obtained in 15th of July 2013, from Zabbix Forums: https://www.zabbix.com/forum/showthread.php?t=21030

MPLSINFO. (s.d.). *MPLS - Brief Overview*. Obtained in 20th of December 2012, from MPLSINFO: http://www.mplsinfo.org/

MUNIN. (s.d.). *Monitoring Tools*. Obtained in 3rd of May 2013, from MUNIN: http://muninmonitoring.org/

NAV (s.d.). *Network Administration Visualized*. Obtained in 3rd of May 2013, from UNINETT: https://nav.uninett.no/

NETDISCO (s.d.). *Network Management Tool*. Obtained in 3rd of April 2013, from NETDISCO: http://netdisco.org/

Olups, R. (2010). *Zabbix 1.8 Network Monitoring*. New York: Packt Publishing.

Silveira, S. A. (2003). *Software Livre e Inclusão Digital*. Arlington : Conrad.

SNMP (s.d.). *Simple Network Management Protocol*. Obtained in 20th of December 2012, from: SNMP: http://www.snmp.org

SLO (2008). *Software livre | o que é?*. ERTE/PT - Equipa de Recursos e Tecnologias Educativas / Plano Tecnológico da Educação). Obtained in 24th of April 2013, from DGIDC: http://softlivre.dgidc.minedu.pt/index.php?option=com_content&task=view&id=13&Itemid=81

Tanenbaum, A. (2003). *Computer Networks*. New Jersey: Pearson Education.

Teixeira, R. (1999). *Redes de Computadores, serviços, administração e segurança*. São Paulo: Makron Books.

Zabbix (s.d.). *Zabbix - The Enterprise-class Monitoring Solution for Everyone*. Obtained in 23th of March 2013, from Zabbix: http://www.zabbix.com