INFORMATION SYSTEMS IN MANAGEMENT

Information Systems in Management (2016) Vol. 5 (3) 326−335

NETWORK MONITORING AND MANAGEMENT FOR COMPANY WITH HYBRID AND DISTRIBUTED INFRASTRUCTURE

DARIUSZ DOLIWA, MARIUSZ FRYDRYCH, WOJCIECH HORZELSKI

Department of Mathematics and Informatics, University of Lodz

The article presents the concept and the description of implementation of the system designed for monitoring and management of a computer network for the large company with a hybrid and distributed infrastructure. The system is based on a Nagios software, a software Multi Router Traffic Grapher, NdoUtils, a relational database management system MySQL, the visualization systems for Nagios (NagVis, NagMap) and a dedicated application that was created for the system, which allows on the presentation of monitored resources.

Keywords: network monitoring, network management, Nagios, SNMP

1. Introduction

Nowadays the computer networks of large enterprises and organizations are often the heterogeneous networks. They combine different technologies, using devices from different manufacturers, running different operating systems. In addition, monitoring and management of the network are not limited to one place, but often require an access to remote locations. In such cases, a single dedicated tool does not fulfill their roles or you need to use several different tools simultaneously, which greatly complicate a network administration and increase its cost (purchasing multiple tools, training employees to use them). In the papers [1] and [2] the authors having regard to these factors, presented a reflection on the functionality that should guarantee a system for managing and monitoring network. These features include: the automation of the monitoring, the ability to adapt to changing solutions used in networks, the ability to operate in many different

environments, the modularity that allows you to select only the necessary components depending on the nature of the monitored network, the intelligent storage, the analysis and visualization of the data, the ability to influence the design of the network, eg. through remote and automated configuration management of network devices. This article presents the concept of building a system that would have the requested features. The system will be based on the platform Nagios [3], which is an open software, developed and thoroughly tested in recent years. At the beginning of the XXI century there have been presented the first proposals [4] relating to the deploying Nagios in a large enterprise environment, due to characteristics such as a scalability, the data security issues, the ability to integrate the standard protocols (eg. SNMP, CMIP) and the monitoring application and device with a "closed" architecture (using the proprietary solutions). Since then, the platform has evolved considerably [5] expanding its capabilities for monitoring a bandwidth usage, a quality of service (QoS), and the notification system that can be integrated with e-mail or alerts in the form of SMS messages. The positive results for Nagios platform elements test [6] decided to choose this system as a basis for building applications presented here.

2. System Requirements

The purpose of our application is to enable the detection of network topology in the company, saving and storing network information in the database, monitoring devices and network connections, management of configuration for devices on the network, reporting on the status of devices and notification of the defined situations related to the detection of irregularities in the network. The application should be modular and include such modules as: a topology discovery module, an information management module, a network monitoring module, a device configuration management module and a reporting module. Each of these modules has to perform a certain function.

The topology discovery module must allow on a periodic detection of network devices, enable editing and acceptance of the correctness of the detected data by the operator and create a visualization of the network topology.

The purpose of the information management module is saving and storing information about the network (the descriptions of a physical location of the branch offices, the network devices, the network connections). This module must contain tool to search for information across the database.

The network monitoring module will be used to a detection of the failure network connections, unavailability of devices, the errors at the interfaces according to the preset level, the changes in the configuration of network devices, the resets of network devices, the current load on the network and must allow the preview parameters of the network devices.

The configuration management module is expected to enable an automatic download of the configuration, the identification of the configuration changes and the storage of historical information about the configuration of devices.

The reporting module must allow to the creation of reports on the monitoring of the system availability and reports according to the selected devices or interfaces in a given period of time, according to the selected parameters (the availability, the CPU load, the memory usage, the errors on interfaces). This module should also handle the notifications about the events occurring in the network.

3. Description of the system concept

The presented system will be based on the platform Nagios, also will use the Multi Router Traffic Grapher (MRTG) [7], the NdoUtils software, the relational database MySQL, the visualization systems for Nagios (NagVis, NagMap) and a dedicated application created for the needs of the system (a presentation of the monitored data).

The system will be equipped with an interface for:

- an access to information about the selected device (automatically collected at defined intervals - by default every 5 minutes),
- carrying out the inspection at the request of the selected device parameters,
- an access to the device configuration,
- a notification in the event of an emergency situation defined on the device,
- an access to historical data.

The subject of monitoring by the system will be the network devices (ie. routers and switches (Fig. 1)) and the network services running on selected hosts.

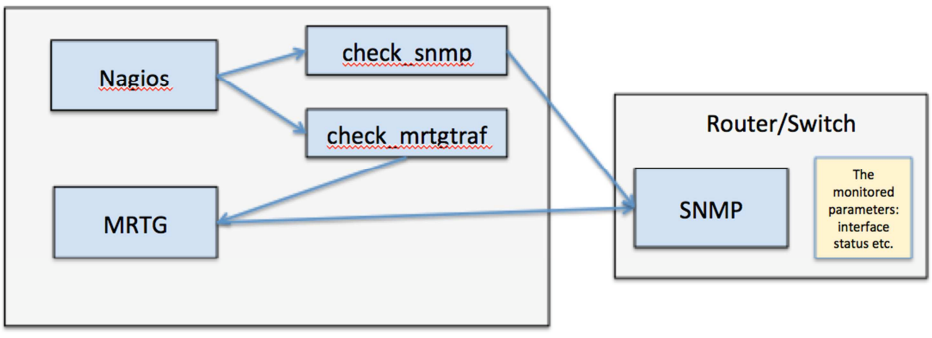


Figure 1. Switch/routers monitoring

The system will be maintained on a single machine, on which will be running:

- Nagios software - to monitor critical IT infrastructure components, including system metrics, network protocols, applications, services, servers, and network infrastructure.
- SNMPTRAPD - an SNMP application that receives and logs SNMP TRAP and INFORM messages.
- SNMPTT - an SNMP trap handler for use with the NET-SNMP/UCD-SNMP snmptrapd program. Received traps are translated into friendly messages using variable substitution. Output can by to MySQL (Linux/Windows) or any other ODBC database.
- Database Server.

4. The topology discovery module.

The purpose of this module is to detect changes in the network topology by adding the new device and to gather information about the device. After detecting the new device, the system will allow to add information about it to the database. Detecting hosts will be able to take place periodically or on demand. After scanning the system prepares a list of the active devices, and then tries to get information about an appropriate facility.

Detection of new devices in the system will be based on the use of network scanner Network Mapper (Nmap). The operator will set out a range of addresses to search.

Additional, the detection of neighbouring devices will be based on the protocols:

- Cisco Discovery Protocol (CDP) (for Cisco devices)
- Link Layer Discovery Protocol (LLDP) (in other cases)

5. Data Storage

The application will consist of three databases implemented using relational database management system MySQL (Fig. 2) :

- the first database (a configuration database) will contain the configuration information for the system;
- the second database (the NdoUtlis database, the database of current states) will base on data generated by the plug-in NdoUtils with the current values of the monitored parameters;
- the third database (a capacitance database) will be gathering historical information of the monitored parameters, allowing for their analysis in selected time intervals and stores the configuration files of monitored devices (current and historical).

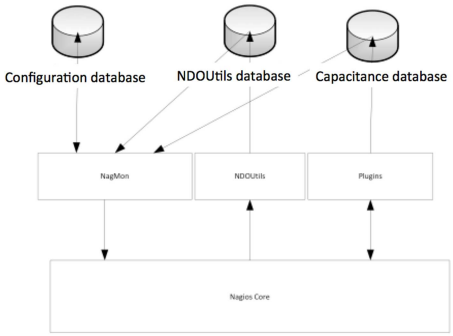


Figure 2. System databases

The configuration database will hold:
- a system configuration: the directories used by the system (the system installation site, the location of system configuration files and the data files, a directory for temporary data); the parameters related to the security of access to the system; the communication parameters (devices addresses and ports services);
- the system user accounts: the system will have defined the user accounts and the ability to group users; a database will store information about existing accounts containing data such as user id, its name, personal details and address, email address and telephone number (to allow to inform the user about the specified events);
- the information about the monitored locations (location id, name, alias, address, GPS coordinates);
- the information on the monitored devices (hosts): name, alias, device type, model, IP address, user and password for SNMP, monitoring intervals, notification parameters relating to changes in device status (period and frequency of notifications) defined on the device "traps" (as described);
- the monitored services (virtual objects, with which to gather information); it is assumed for that host will be possible to define the services monitored on the device; for most devices there will be represented device interfaces status and the use of bandwidth for the interface; for each of the sites there will be determined the name of the device on which the service is monitored and the monitoring parameters (interval monitoring, notification)
- the information about the network connections: operator id, operator name, alias, address, description of the link, bandwidth of the link.
The largest part of the configuration database will occupy descriptions of the equipment and monitored on their services.

The current states database will periodically copy information generated by Nagios (using plug-in NdoUtils) and Multi Router Traffic Grapher, and gather the

device configuration files when it detects the changes in the monitored devices (using "trap" SNMP and TFTP protocol).

The capacitance database will be gathering historical information of the monitored parameters and storing the archived configuration files of the monitored devices.

To support databases there will be delivered applications to manage them with a friendly and easy-to-use graphical interface.

6. The monitoring module

The monitoring module will be responsible for periodic collection of information about the devices and placing them in the appropriate database. For its implementation will be used NagiosCore, plug-in NdoUtils and monitor MRTG. The parameters necessary for the proper functioning of the system Nagios will be stored in the appropriate configuration files are generated automatically based on the data stored in previously described databases.

The definition of each service will be preceded by the definition of the host (the network device) to which it relates.

For each service we must specify the frequency of monitoring, the system operator may also perform the test on demand. The Nagios Core has dozens of commands based on built-in plug-ins for monitoring services. In our system it is planned to use the following commands:

- *check_host_alive* – command allows us to control the availability of host on the network;
- *check_interface_alive* – komenda pozwalająca nam monitorować dostępność portu;
- *check_snmp* - command allows us to read any parameter values for the device using SNMP;
- *check_snmp_getinterfacedata* – command allows us to connect to the specified host and retrieve the status of all meters and status for all interfaces;
- *check_snmp_device_status* – command allows us to download from a designated host data on utilization of CPU and RAM;
- *check_snmp_backup_config* - command allows us to backup the configuration of the network device.

Using these commands, the application collects relevant information that then using the information management module are stored in the respective database and can be displayed to the system operator.

The monitoring module in addition to the polling specified parameters will also support events on those devices. This will be done through the SNMP service. SNMP traps enable a monitored device to notify the management station of significant events by way of an unsolicited SNMP message. The configuration database includes defined for monitored devices "traps" and the critical values which will lead to the generation of a message by the device. Presented module will receive SNMP traps sent from the network equipment and will be responsible for their interpretation and activate alerts the appropriate users. It is assumed that the server where the system is installed will will have running the following services: snmptrapd and snmptt. At a time when the device will generate a trap signal it will be sent to the server snmptrapd. The server sends snmptrapd traps to snmptt parser that parses the information received and take appropriate action (Fig. 3).

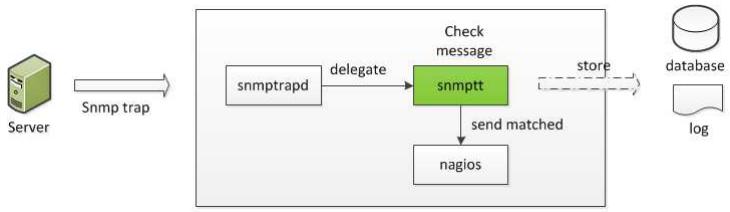


Figure 3. Connection between Nagios and SNMP traps

The monitoring module also allows us to analyze the amount of data flowing through the network devices via NetFlow protocol (this applies to devices that support NetFlow protocol). The service which is responsible for receiving NetFlow data, periodically or at the request of the operator, activates or deactivates the respective collectors. The data thus obtained will be analysed through created for this purpose graphical interface.

7. The configuration management module

This module simplifies managing network configuration files in network environments by continuously monitoring device configurations and providing immediate notification of configuration changes. Automatically store full device configurations in text file format that can easily be restored or copied to set up a new device. We can view, track, and compare configurations with a Web-based graphical interface. This module allows as to immediately rollback to a previous known good device configuration. Configuration Manager establishes communication with the devices via SSH / Telnet / SNMP to check the configuration. The configuration files are transferred from and to the monitored

device using TFTP protocol. The devices in the inventory can be grouped based on any logical criteria - for example Cisco_Switch Group containing all Cisco switches. Configuration operations such as backing up configuration, uploading configurations to devices and others can be performed on all devices of the group at one go. The configuration monitoring engine can be operated manually by user request or run automatically on specific dates and times. It can provides automatic actions such as executing commands, sending SNMP traps or email notifications on specific configuration changes. It can also provides reporting, logging and exporting capabilities that can be used for enhanced management of current and historical network devices configuration.

8. The reporting and visualisation module

The visualisation module will provide an interface for this system, its task will be to visualize the data collected from relevant databases in order to illustrate the current status of devices and network services. The application interface will be divided into an informative part (visualization for active/passive monitoring and monitoring "on demand"), the detection module management and device configuration management.

Informational part of the interface will offer views of the monitored network with varying degrees of detail:

- in the general review will be presented to the condition of the connections between locations, with summary status of the devices in location (NagVis can be used to visualize Nagios data);
- an overview of the selected location will show the status of hosts in a given location (Fig. 4);

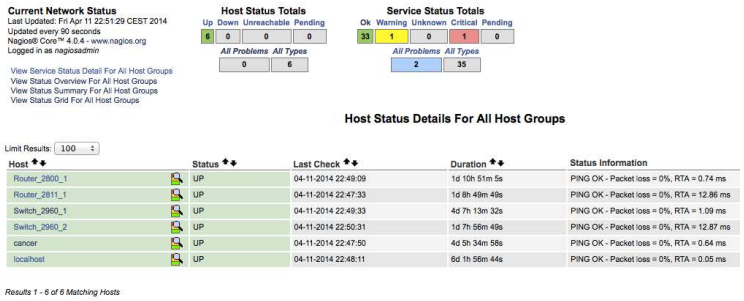
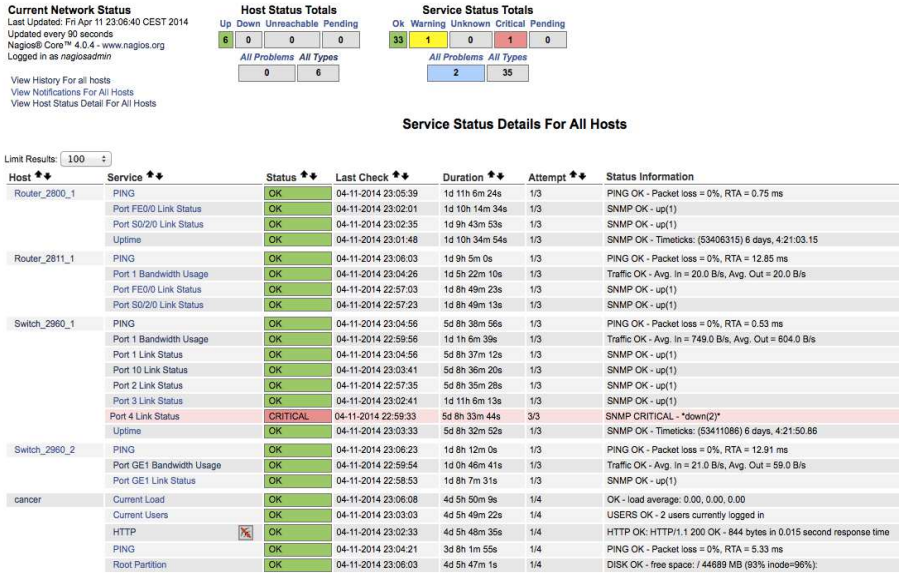


Figure 4. Review of hosts status

- a detailed view for the selected host (Fig. 5);



Current Network Status
Last Updated: Fri Apr 11 23:06:40 CEST 2014
Updated every 90 seconds
Nagios® Core™ 4.0.4 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
6	0	0	0

All Problems	All Types
0	6

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
33	1	0	1	0

All Problems	All Types
2	35

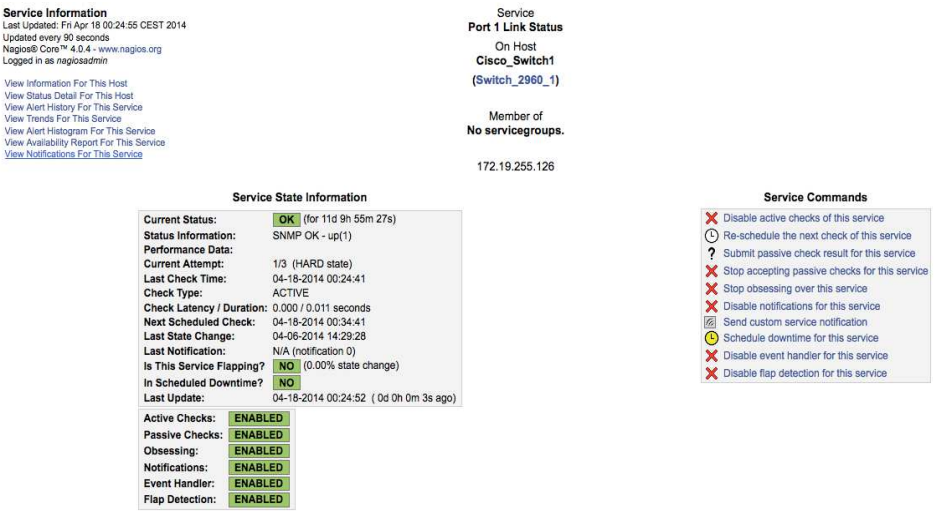
Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Router_2800_1	PING	OK	04-11-2014 23:05:39	1d 11h 6m 24s	1/3	PING OK - Packet loss = 0%, RTA = 0.75 ms
	Port FE0/0 Link Status	OK	04-11-2014 23:02:01	1d 10h 14m 34s	1/3	SNMP OK - up(1)
	Port S0/2/0 Link Status	OK	04-11-2014 23:02:35	1d 9h 43m 53s	1/3	SNMP OK - up(1)
	Uptime	OK	04-11-2014 23:01:48	1d 10h 34m 54s	1/3	SNMP OK - Timeticks: (53406315) 6 days, 4:21:03.15
Router_2811_1	PING	OK	04-11-2014 23:06:03	1d 9h 5m 0s	1/3	PING OK - Packet loss = 0%, RTA = 12.85 ms
	Port 1 Bandwidth Usage	OK	04-11-2014 23:04:26	1d 5h 22m 10s	1/3	Traffic OK - Avg. In = 20.0 B/s, Avg. Out = 20.0 B/s
	Port FE0/0 Link Status	OK	04-11-2014 22:57:03	1d 8h 49m 23s	1/3	SNMP OK - up(1)
	Port S0/2/0 Link Status	OK	04-11-2014 22:57:23	1d 8h 49m 13s	1/3	SNMP OK - up(1)
Switch_2960_1	PING	OK	04-11-2014 23:04:56	5d 8h 38m 56s	1/3	PING OK - Packet loss = 0%, RTA = 0.53 ms
	Port 1 Bandwidth Usage	OK	04-11-2014 22:59:56	1d 1h 6m 39s	1/3	Traffic OK - Avg. In = 749.0 B/s, Avg. Out = 604.0 B/s
	Port 1 Link Status	OK	04-11-2014 23:04:56	5d 8h 37m 12s	1/3	SNMP OK - up(1)
	Port 10 Link Status	OK	04-11-2014 23:03:41	5d 8h 36m 20s	1/3	SNMP OK - up(1)
	Port 2 Link Status	OK	04-11-2014 22:57:35	5d 8h 35m 28s	1/3	SNMP OK - up(1)
	Port 3 Link Status	OK	04-11-2014 23:02:41	1d 11h 6m 13s	1/3	SNMP OK - up(1)
	Port 4 Link Status	CRITICAL	04-11-2014 22:59:33	5d 8h 33m 44s	3/3	SNMP CRITICAL - *down(2)*
	Uptime	OK	04-11-2014 23:03:33	5d 8h 32m 52s	1/3	SNMP OK - Timeticks: (53411086) 6 days, 4:21:50.86
Switch_2960_2	PING	OK	04-11-2014 23:06:23	1d 8h 12m 0s	1/3	PING OK - Packet loss = 0%, RTA = 12.91 ms
	Port GE1 Bandwidth Usage	OK	04-11-2014 22:59:54	1d 0h 46m 41s	1/3	Traffic OK - Avg. In = 21.0 B/s, Avg. Out = 59.0 B/s
	Port GE1 Link Status	OK	04-11-2014 22:58:53	1d 8h 7m 31s	1/3	SNMP OK - up(1)
cancer	Current Load	OK	04-11-2014 23:06:08	4d 5h 50m 9s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	04-11-2014 23:03:03	4d 5h 49m 22s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	04-11-2014 23:02:33	4d 5h 48m 35s	1/4	HTTP OK: HTTP/1.1 200 OK - 844 bytes in 0.015 second response time
	PING	OK	04-11-2014 23:04:21	3d 8h 1m 55s	1/4	PING OK - Packet loss = 0%, RTA = 5.33 ms
	Root Partition	OK	04-11-2014 23:06:03	4d 5h 47m 1s	1/4	DISK OK - free space: / 44689 MB (93% inode=96%):

Figure 5. Detailed view for selected hosts

- a detailed view of the selected service (Fig. 6).



Service Information
Last Updated: Fri Apr 18 00:24:55 CEST 2014
Updated every 90 seconds
Nagios® Core™ 4.0.4 - www.nagios.org
Logged in as *nagiosadmin*

View Information For This Host
View Status Detail For This Host
View Alert History For This Service
View Trends For This Service
View Alert Histogram For This Service
View Availability Report For This Service
View Notifications For This Service

Service
Port 1 Link Status
On Host
Cisco_Switch1
(Switch_2960_1)

Member of
No servicegroups.

172.19.255.126

Service State Information

Current Status:	OK (for 11d 9h 55m 27s)
Status Information:	SNMP OK - up(1)
Performance Data:	
Current Attempt:	1/3 (HARD state)
Last Check Time:	04-18-2014 00:24:41
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.011 seconds
Next Scheduled Check:	04-18-2014 00:34:41
Last State Change:	04-06-2014 14:29:28
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	04-18-2014 00:24:52 (0d 0h 0m 3s ago)

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

Service Commands

- Disable active checks of this service
- Re-schedule the next check of this service
- Submit passive check result for this service
- Stop accepting passive checks for this service
- Stop obsessing over this service
- Disable notifications for this service
- Send custom service notification
- Schedule downtime for this service
- Disable event handler for this service
- Disable flap detection for this service

Figure 6. Detailed view for selected service

9. Summary

Presented here concept of a monitoring system allows us to build an efficient monitoring application for LAN and WAN networks using tools based on open source software. The proposed solutions allow scalability of such a system, which can be used in small, medium and large enterprises. The system does not have high hardware requirements. This allows us to keep costs low for both: its creation and implementation in the enterprise. Described here solutions have been installed, configured and tested in a laboratory environment.

REFERENCES

[1] Sihyung Lee, Kyriaki Levanti, Hyong S. Kim, Network monitoring: Present and future; Computer Networks,Volume 65, 2 June 2014, Pages 84–98;

[2] David Padi, Telecommunications & Information Technology Network Management, challenges in acquisition, design and systems development, NGNS'2009: 2nd International Conference on Adaptive Science & Technology pp 52-53;

[3] Nagios manual: http://library.nagios.com/library/products/nagioscore/ manuals/

[4] Carson Gaspar, Deploying Nagios in a Large Enterprise Environment, at USENIX LISA '07 (presentation on 21st Large Installation System Administration Conference, November 2007, Dallas, Texas)

[5] Mohd Shuhaimi, Roslan, I., Zainal Abidin, Z., Anawar, S.; The new services in Nagios: Network bandwidth utility, email notification and sms alert in improving the network performance, Information Assurance and Security (IAS), 2011 7th International Conference

[6] Ahmed Dooguy Kora, Moussa Moindze Soidridine, Nagios Based Enhanced IT Management System, International Journal of Engineering Science and Technology (IJEST), Vol. 4 No.03 March 2012, PP: 1199-1207

[7] MRTG configuration reference: http://oss.oetiker.ch/mrtg/doc/mrtg-reference.en.html