Simple Network Management Based on PHP and SNMP

Krasimir Trichkov, Elisaveta Trichkova

Abstract: *This paper aims to present simple method for network management based on SNMP - management of Cisco router. The paper examines communication and management of network hardware with php and SNMP.*

Key words: *Network management; Router; PHP; SNMP.*

INTRODUCTION

Nowadays fast developing information technologies make networks more and more complex. Network management is a critical solution to enhance the administrative productivity. Network management means different things to different people. In general, network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks.

In this paper, some fundamental knowledge for network management and the fundamental concepts of SNMP are reviewed. A model for network management is presented. This model describes the goal of network management and is applicable for most modern network management protocols including SNMP.

The heart of the network management system is a set of applications that meet the needs for network management. At a minimum, a system will include basic applications for performance monitoring, configuration control, and accounting. Sophisticated systems will include more elaborate applications in those categories, plus facilities for fault isolation and correction, and for managing the security features of the network.

NETWORK MANAGEMENT MODEL

Figure 1 shows a model for network management. In this model, the network consists of several devices that have a management agent running in them. The management agent has knowledge of the device parameters it runs on. Some of the device parameters are specific to the device that is managed. For instance, router devices will have parameters that describe the routing table. All devices can be expected to have some common parameters such as the name of device, how long the device has been active (up time), and so on.

Figure 1 shows that the agents can be managed by a special device called the Network Management Station (NMS). The Network Management Station can issue specific requests to a device for information about its network parameters. The agent for the device will receive these requests, and send back the requested information. The Network Management Station, upon receiving the reply, knows the value of the requested parameters. It can use this information to deduce information on the state of the device and whether the device requires attention.

It might also be important to prevent an unauthorized Network Management Station from obtaining information on the devices on the network. This requires that some authentication scheme be implemented that will prevent unauthorized access. [1]

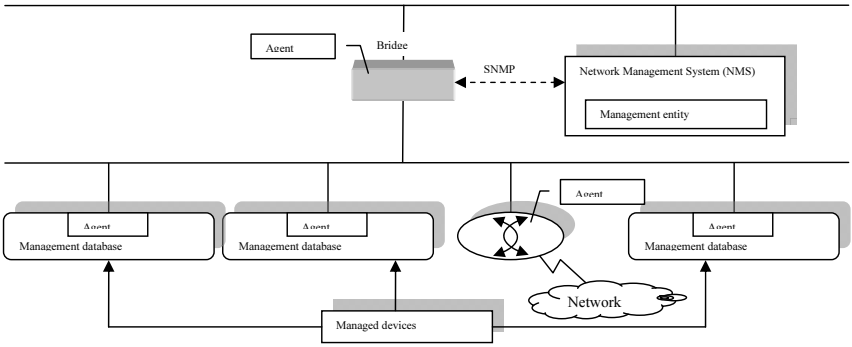

Fig. 1. Model for network management

BASIC GOAL OF NETWORK MANAGEMENT

Figure 2 shows the goal of network management. The network is shown as a "cloud" that has both input and output. The network input is the shared data and the activity generated by users of the network. The network output is the increased efficiency that results from information sharing. The network is subject to disturbances in the form of computers, devices and network links becoming in operational. The goal of network management is to monitor the status of the network, and use control mechanisms to achieve the desired output (increased efficiency) despite the network disturbances.

The mechanisms used for monitoring and controlling the network should be such as to have a minimal impact on the network. In other words, the protocols used to collect information should not impact the performance of the network and the devices that are managed. If the network management mechanism uses up most of the network bandwidth, very little will be available for the network users. In this case the network traffic will be disrupted or the network will slow down because user network traffic must compete with network management traffic for bandwidth. The network agents running on the devices should not consume a great deal of processing power on their devices; otherwise, the device may not be able to perform its normal functions in the desired time. [1]

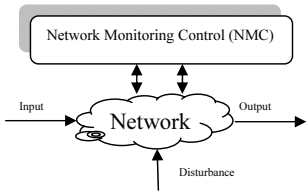

Fig. 2. The goal of network management

MANAGEMENT INFORMATION BASE (MIB)

The parameters in the managed node are called management objects. The set of these management objects is called the Management Information Base (MIB). MIB is a type of database used to manage the devices in a communications network. It is a hierarchical database that defines the information that an SNMP management system can request from an agent using SNMP.

The managed devices in a communications network are called objects and they are a logical representation of physical networking components that are SNMP-enabled (e.g. computers, hubs, switches and networking software). MIB collects all possible objects in a network and contains information about the configuration of these networking components (e.g. the version of the software running on the component, the IP address and port number, the amount of available disk space for storage).

MIB role is a type of directory, which contains the logical names of the network resources and their configuration parameters managed by SNMP.

SNMP MANAGEMENT PARADIGM

The Network Management Station for SNMP is called the SNMP Manager. The SNMP Manager uses a management paradigm that is called the remote debugging paradigm (see Figure 3). In this paradigm, the SNMP Manager is similar to a programmer at a workstation debugging programs from a remote location. Such a hypothetical programmer would be interested in reading the values of variables in the program and changing the values of certain critical variables. Likewise, the SNMP Manager should be able to read and update values of MIB variables on the managed devices. The SNMP Manager should be able to perform the following actions:

- Read or read-write of MIB variables
- Trap-directed polls
- Simple traversal of variables in the managed node

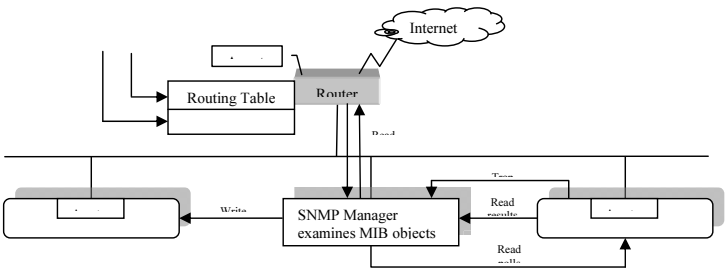

Fig. 3. SNMP Manager Paradigm

When an exceptional condition occurs at a managed device, such as failure of a link or a critical change in status of a device, the managed device sends a trap SNMP message to the SNMP Manager. The trap message contains an indication of the event that caused the generation of the message. It is up to the SNMP Manager to respond to the trap message. The SNMP Manager can simply log the message in a trap log file, or take more action that is extensive. The SNMP Manager can, for instance, request additional information from the device that generated the trap message. The additional information can be obtained through read requests for specific MIB variables. If the SNMP Manager is programmed for control of the device, it can issue a write request to modify the value of a MIB variable.

All control actions within SNMP occur as a "side effect" of modifying a MIB variable. For example, if a device is to be powered-off remotely from an SNMP Manager, the SNMP Manager could send a write request to modify a MIB variable called the ifPowerOn variable. The managed device can be programmed so that the ifPowerOn variable causes the following side effect: the value of the variable is normally 1; if the value is 0, the device will be powered off. The managed device, upon sensing a value of 0 in its ifPowerOn variable, can initiate a device shutdown.

Because the MIB variables are ordered according to their object identifiers, the SNMP manager can traverse all the variables in the device using an SNMP command called GetNext. This is called a simple traversal of the MIB.

Because SNMP uses side effects to initiate control actions, the SNMP commands consist of only the following:

- Get (Read a MIB variable)
- Set (Write a MIB variable)
- GetNext (Return the next MIB variable)

- Trap (Sent to SNMP manager to report exceptional conditions)

Note that the terms trap and event are synonymous because the occurrence of an SNMP event generates an SNMP trap message. [2]

SAMPLE OF MANAGEMENT OF CISCO ROUTER

Figure 4 shows abstract model of Web Service. It demonstrates the implementation of network services, which can be invoked both from a workflow orchestration engine and through graphical user interface. The role of the mediation device is related with the automatic interfacing and invocation of network information services, but the triggering of these services is performed from an object, belonging to workflow execution architecture. [3]

The mediation architecture is connected into three tiers functional scheme of workflow execution, including automatic service invocation for the networked elements:

- workflow engine and/or graphical user interface;
- mediation device to perform the automatic functionality for service invocation and results communication to and from the network technical elements;
- the network technical elements, which are managed by the workflow engine.

The web service is developed for the case of management of routes services. The lasts are defined as user available Web services, which can be automatically called by workflow engine.

The sequence of operation and the invocation of the network services with mediation devices are explained as follows.

A Client, as part of the workflow sequence, invokes a network service. The network services are formalized with WSDL (Web Service Description Language) description, related for the implementation of a set of Router Web Services.

Client of the workflow applications sends and SOAP Request messages to the network Router Web Services.

The Mediation device is responsible for the transmission of the parameters of the Requests to the network Router Web Services.

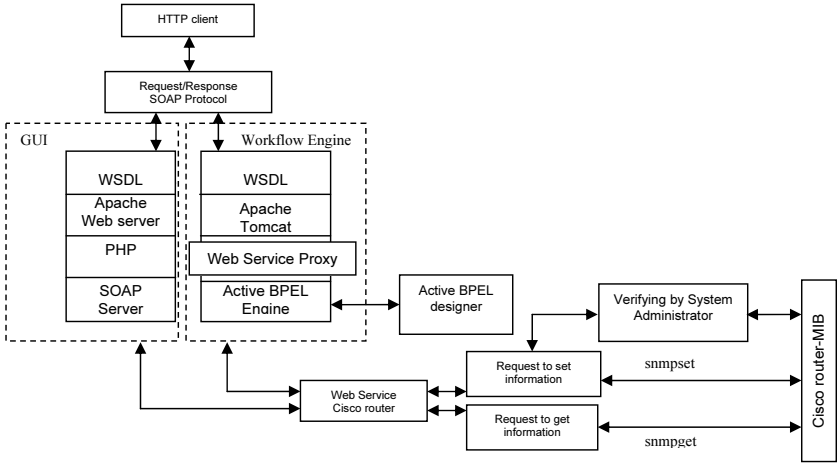

Fig. 4. Common client/server architecture

Currently the Mediation device is implemented to support the following working algorithm:

- With respect to the internal router functionalities, the mediation device can directly perform tuning of the router parameters. These operations are implemented using

the SNMP management protocol and MIB (Management Information Base) of router. For example: to view IP route, mediation device using snmp and router's MIB sends - snmpget ("$host","$community",".1.3.6.1.2.1.4.21.1.7.0.0.0.0"). The host is local router address (192.168.0.1), community string is "public", and ".1.3.6.1.2.1.4.21.1.7.0.0.0.0" is description in router MIB of this operation (IP route). To stop IP address, mediation device sends: snmpset("$host", "$community",".1.3.6.1.2.1.2.2.1.7.9","i","2"). The ".1.3.6.1.2.1.2.2.1.7.9" describes that this operation will stop IP with number 9 (the last digit), "i" presents "integer, and "1" - the status (1-up, 2-down).

- For the case when the internal router functionalities don't allow automatic and/or SNMP management (for example for security or MIB reasons), man-machine interface has to be applied. In this case the mediation device sends an E-mail to the system administrator for the invocation of a set of commands trough a Command Line Interface, supported by the network device. For example: to make NAT (Network Address Translation) or open port in firewall.

After the implementation of the network operations, the results, generated by the network devices are sent to the Mediation devices. The last then defines a respond message to the client. Following the workflow architecture of the workflow engine, a Send SOAP Response messages is directed to the client.

In the end the Client receives, the SOAP Response messages and following the modelled workflow choreography can perform new network service and to resubmit new message towards the network router Web Services.

CONCLUSIONS AND FUTURE WORK

Network management is a critical solution to enhance the administrative productivity. Network management is to maintain and optimize the operation of networks that includes mainly monitoring and modifying the functions of networks. In this paper, some fundamental knowledge for network management and the fundamental concepts of SNMP are reviewed. A model for network management is presented. This model describes the goal of network management and is applicable for most modern network management protocols including SNMP.

REFERENCES

[1] http://www.microsoft.com/technet/archive/winntas/maintain/networkm.mspx?mfr=

[2]http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800aea9c.shtml

[3] Elisaveta Trichkova, Krasimir Trichkov, Elena Ivanova, Web Service Integrated System and Basic Security Concepts. International Conference Automatics and Informatics' 07, October 3-6, 2007, Sofia, Bulgaria, VI-43 - VI-46.

Contacts:

Assist. Prof. Krasimir Trichkov, Department Hierarchical Systems, Institute of Computer and Communication Systems – BAS, phone: (359 2) 979 2774, e-mail: krasi@hsi.iccs.bas.bg

Assist. Prof. Elisaveta Trichkova, Department Hierarchical Systems, Institute of Computer and Communication Systems – BAS, phone: (359 2) 979 2774, e-mail: elisaveta@hsi.iccs.bas.bg

This paper is supported by the project: Creative Development Support of Doctoral Students, Post-Doctoral and Young Researches in the Field of Computer Science, BG 051PO001-3.3.04/13, European social fund 2007–2013r. Operational programme "human resources development"

The paper has been reviewd.