WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Network Operation and Management

Assistant Prof. Ms. Kalpana N. Rode, Mr. Om S. Hattarki, Mr. Suryavardhan S. Nerle

Electronics &Telecommunications Engineering Department, Sharad Institute of TechnologyCollege of Engineering, Yadrav, Ichalkaranji, India
omhattarki13@gmail.com

ABSTRACT:

In this paper we present a newly begun research project about the performance evaluation of network management operations using static and mobile agent approach. The general objectives of this research project are to study using simulation the behaviour of performance of a range of network management concepts in order to find out their operation under a number of different situations. The expected outcome of this project is to provide recommendations on the appropriateness of different agent designs for different network management operations in different circumstances, specifications of management information required supporting these agents, and identification of the protocol and operational requirements necessary to support mobile network management agents.

INTRODUCTION:

Nowadays, network and distributed processing systems are of critical and growing importance in enterprises of all sorts. The trend is toward larger, more complex networks supporting more applications and more users. Network Management is critical to meeting the needs and demands of this complexity. Leinwand and Conroy [1] defined Network Management as a procedure of managing a complex data network to make the most of its efficiency and productivity. There are some known drawbacks of existing network management frameworks including insufficient scalability, interoperability, reliability and flexibility as networks become more geographically distributed. It is apparent that Network Management needs to be addressed in particular performance issues associated with a distributed computer network (in respect of a variety of heterogeneous devices, traffic types and performance demand) to meet expectations on efficiency and productivity. II. NETWORK MANAGEMENT PROBLEM At present, most network management systems operate

A network management system (NMS) is an application or set of applications that lets network engineers manage a network's independent components inside a bigger network management framework and performs several key functions. An NMS identifies, configures, monitors, updates and troubleshoots network devices -- both wired and wireless -- in an enterprise network. A system management control application then displays the performance data collected from each network component, allowing network engineers to make changes as needed.

Network element vendors make their performance data available to NMS software either through APIs or through a protocol such as NetFlow, a de facto industry standard originally developed by Cisco that allows NetFlow-enabled routers to transmit traffic and performance information.

Network technique is a technique for planning, scheduling (programming) and controlling the progress of projects. This is very useful for projects which are complex in nature or where activities are subject to considerable degree of uncertainty in performance time.

This technique provides an effective management, determines the project duration more accurately, identifies the activities which are critical at different stages of project completion to enable to pay more attention on these activities, analyse the scheduling at regular interval for taking corrective action well in advance, facilitates in optimistic resources utilisation, helps management for taking timely and better decisions for effective monitoring and control during execution of the project.

Network Monitoring Techniques

Ping monitoring

Network pings are one of the oldest monitoring techniques, but it is still widely used by NPMs today. The monitoring tool sends a packet (or multiple packets) to a node or device, expecting to receive a response back. If the target node sends back an “all-clear” message, the monitor knows the node is up-and-running. However, if no response is received, it sends out more pings to get the node’s attention. If these pings still turn up nothing, the monitoring tool alerts the user. Pings are a relatively simple monitoring technique, but are still a great way for enterprises to examine if devices are currently running.

Log file monitoring

Typically, devices on a network will generate log files as they operate. These log files provide basic information that the device can report on, including any errors. While it isn't as sophisticated as other techniques, some tools monitor log files to look for device-reported troubles. Log files are simple text files that might contain keywords such as "error" or "critical" that signal a problem with the node. Monitoring tools look for these keywords and report on anything unusual.

SNMP monitoring

Most devices nowadays are compliant with SNMP, or Simple Network Management Protocol. SNMP is a device protocol that provides monitoring tools and nodes a common language to communicate with each other. The system relies on agents inside devices to provide information to network managers and monitoring tools. An SNMP manager sends out polls to devices to inquire about their current status, and devices can send traps when significant network events occur. NPMs that include SNMP monitoring have a common framework to talk to each other, centralizing and simplifying monitoring capabilities.

NetFlow monitoring

NetFlow systems use packet traps to examine traffic that passes through a part of the network. The NetFlow probes capture traffic data and then sends it to a monitoring tool for analysis. The analysis examines network traffic flow and volume to determine how data moves through the network. Flow-based monitoring systems, including NetFlow, analyze the conversations between devices and ensures that data and information is travelling along the network path smoothly.

SQL query monitoring

To monitor databases connected to a network, monitors can utilize SQL queries. These queries ask the database to provide information on the number of data requests, transmissions, etc. Using this information, a monitor can determine if the database is performing adequately or not. Ideally, the database should be sending data across a network to accommodate for every request it receives; if the database is performing slowly, the monitoring tool can detect it and inform the network team.

Network Management Architecture

Interactions within network management may include interactions among components of the management system; between the network management system and network devices; and between the network management system and the OSS.

If there are multiple network management systems, or if the network management system is distributed or hierarchical, then there will be multiple components to the management system. The network architecture should include the potential locations for each component and/or management system, as well as the management data flows between components and/or management systems. The interactions here may be in the form of SNMP or CMIP/CMOT queries/responses, CORBA, HTTP, file transfers, or a proprietary protocol.

Part of network management inheres in each managed network device, in the form of management data (e.g., MIB variables) and software that allows access and transport of management data to and from the management system (e.g., SNMP agent software). Therefore, interactions between network management components (particularly monitoring devices) and managed network devices can also be considered here. We may choose to consider all of the managed network devices, depending on how many of them are expected in the network; however, we usually do not consider all managed devices in the network, as there can be quite a large number of them. As we discussed in flow analysis (Chapter 5), the devices that are most likely to be considered are those that interact with several users, such as servers and specialized equipment. Interactions here are likely to be in the form of SNMP or CMIP/CMOT queries/responses.

If your environment includes an OSS, there will likely be some interactions between network management and the OSS, for flow-through provisioning, service management, and inventory control. The network management architecture should note where the OSS would be located, which components of the network management system will interact with the OSS, and where they will be located in the network. Interactions here are likely to use CORBA, but may use SNMP or HTTP .

CONCLUSIONS:

This paper has presented an efficient and automatic network monitoring and management system which quickly reports to network administrator in case of any problem. Nagios is configured to generate and monitor the whole network topology and send notifications in case of state change anywhere in the network. These notifications will generate tickets in RT. The further network management task is performed by RT. RT is configured to send email or International Journal of Information and Electronics Engineering, Vol. 3, No. 1, January 2013125

sms to all responsible persons one by one after every pre-defined time interval until the problem is solved. This network monitoring system is fully

automatic and the administrator has to check only his emails. The presented network monitoring system is intelligent to quickly identify problem location in the network and also its effect on the rest of the network. Thus, it is highly efficient and provides full control over the network.

REFERENCES:

1. D. Ten, S. Manickam, S. Ramadass, and H. A. Bazar, "Study on Advanced Visualization Tools In Network Monitoring Platform," in Third UKSim European Symposium on Computer Modeling and Simulation, EMS '09', Minden Penang, Malaysia, December 2009.
2. L. Chang, W.L. Chan, J. Chang, P. Ting, M. Netrakanti, "A network status monitoring system using personal computer," presented at IEEE Global Telecommunications Conference, August 2002.
3. R. Talpade, G. Kim, and S. Khurana, "NOMAD: traffic-based network monitoring framework for anomaly detection," IEEE International Symposium on Computers and Communications vol. 9,Morristown, NJ, August 2002.
4. S. Feng, J. Zhang, and B. Zeng, "Design of the Visualized Assistant for the Management of Proxy Server," presented at IEEE Third International Symposium on Electronic Commerce and Security (ISECS), Wuhan, China, August 2010.
5. X. Wang, L. Wang, B. Yu, and G. Dong, "Studies on Network Management System framework of Campus Network," presented at 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR), 2010, Yantai, China.