Automatic Troubleshooting and Monitoring of Large Network Systems

Renuka Deshpande [1] Dipali Wagh [2] Amruta Shirode[3] Suleman Tadvi[4]

Departemnt of Computer Engineering SSBT COET,
North Maharashtra University,Jalgaon

Abstract: *Networks are getting larger and more complex, yet administrators depend on rudimentary tools to debug problems. An automated and systematic approach for testing and debugging networks called "Automatic Troubleshooting and Monitoring of Large Network System"(ATML) is proposed to solve the problem of connectivity. The model is used to generate a minimum set of test packets to check the connectivity in the network. Test packets are sent continuously and periodically and detected failures trigger a separate mechanism to localize the fault. ATML forms the group and checks the connection according to the priority assign to them. The connection problem is automatically troubleshoot and monitor by the system using the tools to check connection.*

Keywords: *Networks, Test Packets, Priority, Troubleshoot, Monitors*

1. Introduction

Operating a modern network is not a easy task. Every day network engineers have to wrestle with misconfigure routers, fiber cuts, faulty interfaces, mislabeled cables, software bugs, broken links and many other reasons that cause networks to misbehave, or fail completely. Network engineers search and hunt down bugs using the most rudimentary tools like ping, traceroute and SNMP, and track down root causes using a combination of accrued wisdom and intuition.. Facing this hard problem, network engineers deserve better tools than ping and traceroute. In fact, in other fields of engineering testing tools have been evolving for a long time. Thus, a tool is been introduced called as Automatic Troubleshooting and Monitoring of Large Network System.

.

2. Related Work

It is notoriously hard to debug networks. Every day, network engineers battle with router misconfigurations, fiber cuts, faulty interfaces, mislabeled cables, software bugs, disconnected links, and a many other reasons that cause networks to misbehave or fail completely. Network engineers hunt down bugs using the most rudimentary tools (e.g Ping, traceroute, SNMP) and track down root causes using a combination of accrued wisdom and intuition. Now a days the task of controlling the comm-unication across the network is very difficult. There are many network monitoring tools available today which monitor the network host but which cannot restrict the network access based on the three constraints i.e. time, host and user. All the constraints and access rights of a network user are written in the firewall of a respective Bastion machine. For more security, these rules will have to be written in more than one Bastion machine. In the existing system, a network administrator will have to write all such rules in the firewalls of the respective Bastions separately. The administrator will have to manually reconfigure all such rules when the network users move in the network or they change their position. The administrator will have to be there in the current network for reconfiguring the network i.e., the administrator cannot do this job from a remote site or another place. Also there is always a chance for the misuse of the privileges, by the network users given by the administrator. The administrator may misuse his privilege to access the ports of different server machines in the network using utilities such as SSH, TELNET, FTP.

3.Methodology

The proposed system is for a network to automatically parse router configurations and generate a set of test packets for the network. The administrator can login to the central Bastion and can create the group and add specific clients to it, along with updation and deletion. When a user login to the network, the login information is sent to the Bastion Server and all his access rights are retrieved from the database and are applied on the Bastion Server There are different groups of machines based on the priority connected to the server through a hub or switch. The proposed system is expected to rectify all drawbacks of the existing system. The administrator must be able to troubleshoot and monitor the whole network from a central

ISSN: 2278 – 7798

Bastion. There is a sniffer Program in which sniffer checks every packet in the network and find some unexpected text like (bomb, porn) and detect senders IP and details and send mail or message to administrator. The policies or rules for each user are stored in the central database in the Bastion Server. In the system checking of clients or users whether they are connected or not is done by using *ping* and other server commands **.**

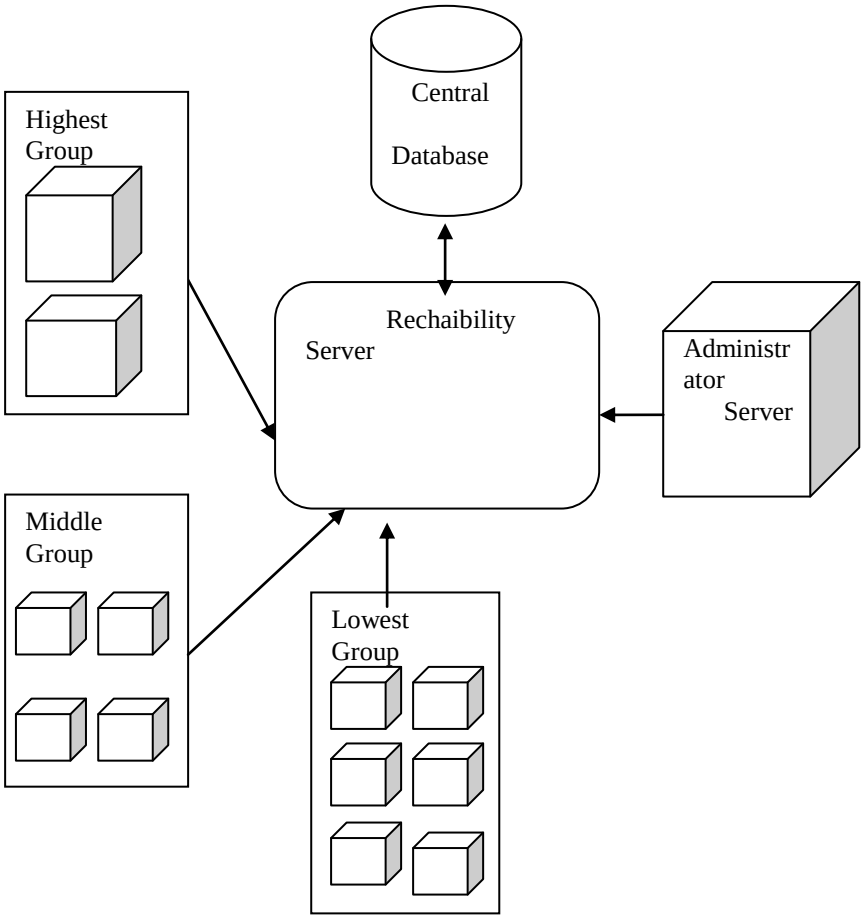

Figure 1 : Block Diagram of ATML

Implementation Plan for Automatic Trouble-shooting and Monitoring of Large Network Systems

1) The system is implemented as a prototype system to automatically parse router configurations and generate a set of test packets for the network.
2) There is a Sniffer Program in which sniffer checks every packet in our network and find some unexpected text like (bomb, porn) and detect senders IP and details and send mail or message to administrator.
3) In this system the program checks whether the clients and users are connected or not in the network using the ping or other server commands
.
4) In the network there are there are some other clients like manager or other users which have continuously connected to network for their work for that user we are setting priority to Check connectivity and report to administrator.
5) The network monitor assumes there are special test agents in the network that are able to send/receive test packets**.** The network monitor reads the database and constructs test packets and instructs each agent to send the appropriate packets**.**
6) All packets are collected in details in the Network and it's log is maintain for sending Test packets using test packet generator.

4.Results

The ATML system is designed to check the connectivity in number of machines by sending test packets periodically through the network and automatically troubleshoots and monitor the Large networks**.**

5. Concluson

Testing liveliness of a network is a fundamental problem for ISPs and large data centre operators. Sending the probes between every pair of edge ports is not exhaustive and not scalable . It suffices to find a minimal set of end-

ISSN: 2278 – 7798

to-end packets that traverse search link. ATML, however, goes much further than liveliness testing with the same framework. ATML can test for Rechaibility policy and performance .Thus Network ATML will be equally useful for automated dynamic testing of production networks.

6.Acknowledgement

This material is based on work supported by Mr. Sushant S. Bahekar, H.O.D of Computer Departement Dr. Prof Girish K. Patnaik From SSBT COET, Jalgaon

7. References

[1] Hongyi Zeng, Peyman Kazemian, George Varghese and Nick McKeown "Automatic Test Packet Generation" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 2, APRIL 2014

[2] P. Kazemian, G. Varghese, and N. McKeown, "Header space analysis: Static checking for networks" in Proc. NSDI, 2012, pp.99

[3] A. Mahimkar, J. Yates, Y. Zhang, A. Shaikh, J.Wang, Z. Ee, and C.T. Ee, "Troubleshooting chronic conditions in large IP networks," in *Proc. ACM CoNEXT*, 2008, pp. 2:1–2:12.
http://eastzone.github.com/atpg/docs/NetDebugSurvey
.pdf

ISSN: 2278 – 7798