ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Detecting functional and Performance issues in a network using Auto Test Packet generation

Ediga Sai Haritha
MTech Student
Department of Computer Science Engineering
Chilukur Balaji Institute Of Technology

P. Dharshan
Associate Professor & HOD,
Department of Computer Science Engineering,
Chilukuri Balaji Institute of Technology.

Abstract: ***Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages. It is part of network management. Commonly measured metrics are response time, availability and uptime, although both consistency and reliability metrics are starting to gain popularity. The widespread addition of WAN optimization devices is having an adverse effect on most network monitoring tools -- especially when it comes to measuring accurate end-to-end response time because they limit round trip visibility. Network tomography is an important area of network measurement, which deals with monitoring the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network/Internet. In this paper we examine and implement an Automatic Test Packet Generation (ATPG) method. This approach gets router configurations and generates a device-independent model. ATPG generate a few set of test packets to find every link in the network. Test packets are forwarded frequently and it detect failures to localize the fault. ATPG can detect both functional and performance (throughput, latency) problems.***

Keywords: ***Automatic Test packet, Ping, Network, Performance.***

Introduction:

In network management terms, network monitoring is the phrase used to describe a system that continuously monitors a network and notifies a network administrator though messaging systems (usually e-mail) when a device fails or an outage occurs. Network monitoring is usually performed through the use of software applications and tools.

At the most basic level, ping is a type of network monitoring tool. Other commercial software packages may include a network monitoring system that is designed to monitor an entire business or enterprise network.

Some applications are used to monitor traffic on your network, such as VoIP monitoring, video stream monitoring, mail server (POP3 server) monitoring, and others. While an intrusion detection system monitors a network for threats from the outside, a network monitoring system monitors the network for problems caused by overloaded and/or crashed servers, network connections or other devices. For example, to determine the status of a webserver, monitoring software may periodically send an HTTP request to fetch a page. For email servers, a test message might be sent through SMTP and retrieved by IMAP or POP3. Status request failures - such as when a connection cannot be established, it times-out, or the document or message cannot be retrieved - usually produce an action from the monitoring system. These actions vary -- an alarm may be sent (via SMS, email, etc.) to the resident sysadmin, automatic failover systems may be activated to remove the troubled server from duty until it can be repaired, etc. Monitoring the performance of a network uplink is also known as network traffic measurement, and more software is listed there.

Route analytics is another important area of network measurement. It includes the methods, systems, algorithms and tools to monitor the routing posture of networks. Incorrect routing or routing issues cause undesirable performance degradation or downtime. Website monitoring service can check HTTP pages, HTTPS, SNMP, FTP, SMTP, POP3, IMAP, DNS, SSH, TELNET, SSL, TCP, ICMP, SIP, UDP, Media Streaming and a range of other ports with a variety of check intervals ranging from every four hours to every one minute. Typically, most network monitoring services test your server anywhere between once-per-hour to once-per-minute.

Monitoring an internet server means that the server owner always knows if one or all of his services go down. Server monitoring may be internal, i.e. web server software checks its status and notifies the owner if some services go down, and external, i.e. some web server monitoring companies check the services status with a certain frequency. Server monitoring can encompass a check of system metrics, such as CPU usage, memory usage, network performance and disk space. It can also include application monitoring, such as checking the processes of programs such as Apache, MySQL, Nginx, Postgres and others.

External monitoring is more reliable, as it keeps on working when the server completely goes down. Good server monitoring tools also have performance benchmarking, alerting capabilities and the ability to link certain thresholds with automated server jobs such as provisioning more memory or performing a backup.

Network monitoring services usually have a number of servers around the globe - for example in America, Europe, Asia, Australia and other locations. By having multiple servers in different geographic locations, a monitoring service can determine if a Web server is available across different networks worldwide. The more the locations used, the more complete is the picture on network availability. When monitoring a web server for potential problems, an external web monitoring service checks a number of parameters. First of all, it monitors for a proper HTTP return code. By HTTP specifications RFC 2616, any web server returns several HTTP codes. Analysis of the HTTP codes is the fastest way to determine the current status of the monitored web server. Third-party application performance monitoring tools provide additional web server monitoring, alerting and reporting capabilities.

Network Design and Key Terminology:

As mentioned in the last section, the automatic test packet generation (ATPG) system makes use of geometric model of header space analysis. This section explains some of the key terms associated with geometric framework of header space analysis.

Packet

Packet in a network can be described as a tuple of the form (port, header) in such a way that, it is the job of port to show position of packet in a network at instantaneous time. Each one of the port is allotted with one and only one unique number.

Switch

Another term used in geometric model of header space analysis is switches. It is the job of switch transfer Function T, to model devices in a network. Example of devices can be switches or routers. There is a set of forwarding rules contained in each device, which decides how the packets should be processed. When a packet comes at a switch, a switch transfer function comperes it with each rule in descending order of priority. If packet does not match withany of the rule then it is dropped. Each incoming packet is coupled with exactly single rule.

Rules

Piece of work for rules is generation of list of one or more output packets associated with those output ports to which the packet is transferred, and explain how fields of port are modified. In other words, rules explains how the region of header space at entrance in changed into region of header space at exit.

Rule History

At any moment, every packet has its own rule history, which can be described as ordered list of rules packet have matched up to that point as it covers the network. Rule history provides necessary and important unprocessed material for automatic test packet generation (ATPG). That is the reason why it is fundamental to ATPG.

Topology

The network topology is modeled by topology transfer function. The topology transfer function gives the specification about which two ports are joined by links. Links are nothing but rules that forwards a packet from source to destination with no modification. If there is not a single topology rule matching an input port, the port is situated at edge of a network and packet has come to its desired destination.

Life of a Packet

One can see life of a packet as carrying out or executing switch transfer function and topology transfer function at length. When a particular packet comes in a network port p, firstly a switch function is applied to that packet. Switch transfer function also contains input port pk.p of that packet. The result of applying switch function is list of new packets [pk1, pk2, pk3,]. If the packet reached its destination it is recorded, and if that is not the case, topology transfer function is used to call upon switch function of new port. This process is done again and again unless packet is at its destination.

Existing System:

- Testing liveness of a network is a fundamental problem for ISPs and large data center operators. Sending probes between every pair of edge ports is neither exhaustive nor scalable . It suffices to find a minimal set of end-to-end packets that traverse each link. However, doing this requires a way of abstracting across device specific configuration files, generating headers and the links they reach, and finally determining a minimum set of test packets (Min-Set-Cover).
- To check enforcing consistency between policy and the configuration.

Disadvantages of Existing System:

- Not designed to identify liveness failures, bugs router hardware or software, or performance problems.
- The two most common causes of network failure are hardware failures and software bugs, and that problems manifest themselves both as reachability failures and throughput/latency degradation.

Proposed System:

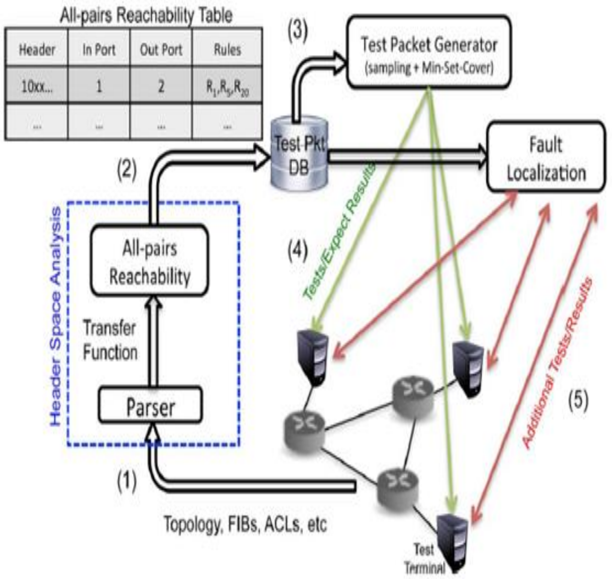
- Automatic Test Packet Generation (ATPG) framework that automatically generates a minimal set of packets to test the liveness of the underlying topology and the congruence between data plane state and configuration specifications. The tool can also automatically generate packets to test performance assertions such as packet latency.
- It can also be specialized to generate a minimal set of packets that merely test every link for network liveness.

Advantages of Proposed System:

- A survey of network operators revealing common failures and root causes.
- A test packet generation algorithm.
- A fault localization algorithm to isolate faulty devices and rules.
- ATPG use cases for functional and performance testing.
- Evaluation of a prototype ATPG system using rule sets collected from the Stanford and Internet2 backbones.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

System Architecture:



The proposed system can be divided into following modules:

- Failures and root causes of network operators
- Data plane analysis
- Network troubleshooting
- ATPG system
- Network Monitor

Failures And Root Causes Of Network Operators

Network traffic is represented to a specific queue in router, but these packets are drizzled because the rate of token bucket low. It is difficult to troubleshoot a network for three reasons. First, the forwarding state is shared to multiple routers and firewalls and is determined by the forwarding tables, filter rules, and configuration parameters. Second, the forwarding state is difficult to watch because it requires manually logging into every box in the network. Third, the forwarding state is edited simultaneously by different programs, protocols and humans.

Data Plane Analysis

Automatic Test Packet Generation framework which automatically generates a minimum set of packets to check the likeness of underlying topology and congruence between data plane state and configuration specifications. This tool can automatically generate packets to test performance assertions like packet latency. ATPG find errors by independently and exhaustively checking all firewall rules, forwarding entries and packet processing rules in network. The test packets are generated algorithmically from the device configuration files and FIBs, with less number of packets needed for whole coverage. Test packets are fed in the network so that every rule is covered directly from the data plane. This tool can be customized to check only for reachability or for its performance

Network Troubleshooting

The cost of network debugging is captured by two metrics. One is the number of network-related tickets per month and another is the average time taken to resolve a ticket .There are 35% of networks which generate more than 100 tickets per month. Of the respondents, 40.4% estimate takes under 30 minutes to resolve a ticket. If asked what is the ideal tool for network debugging it would be, 70.7% reports automatic test generation to check performance and correctness. Some of them added a desire for long running tests to find jitter or intermittent issues, real-time link capacity monitoring and monitoring tools for network state. In short, while our survey is small, it helps the hypothesis that network administrators face complicated symptoms and causes.

ATPG System

Depending on network model, ATPG generates less number of test packets so that every forwarding rule is exercised and covered by at least one test packet. When an error is found, ATPG use fault localization algorithm to ascertain the failing rules or links.

Network Monitor

To send and receive test packets, network monitor assumes special test agents in the network. The network monitor gets the database and builds test packets and instructs each agent to send the proper packets. Recently, test agents partition test packets by IP Proto field and TCP/UDP port number, but other fields like IP option can be used. If any tests fail, the monitor chooses extra test packets from booked packets to find the problem. The process gets repeated till the fault has been identified. To communicate with test agents, monitor uses JSON, and SQLite's string matching to lookup test packets efficiently.

Conclusion:

The network is the lifeblood of any business, so monitoring and optimizing network performance is essential. IT cannot rely on guesswork to successfully execute such an endeavor. Achieving the desired results requires network performance monitoring. Network monitoring tools allow organizations to baseline the network performance of their hardware and software infrastructure. With a baseline of nominal operations in hand, IT is positioned to recognize and respond to conditions that can negatively impact network performance and threaten the user community's productivity and quality of experience. In the present System it uses a method that is neither exhaustive nor scalable. Though it reaches all pairs of edge nodes it could not detect faults in liveness properties. ATPG goes much further than liveness testing with same framework. ATPG could test for reachability policy and performance measure. Our implementation also enlarges testing with simple fault localization scheme also build using header space framework.

References:

[1] Zeng , Kazemian, Varghese,and Nick "Automatic Test Packet Generation",VOL. 22, NO. 2, APRIL 2014

[2] Y. Bejerano and R. Rastogi, "Robust monitoring of link delays and faults in IP networks," IEEE/ACM Trans Netw., vol. 14, no. 5, pp. 1092–1103, Oct. 2006

[3] N. Duffield, "Network tomography of binary network performance characteristics," IEEE Trans. Inf. Theory,vol. 52, no. 12, pp. 5373–5388, Dec. 2006.

[4] N. Duffield, F. L. Presti, V. Paxson, andD.Towsley,"Inferringlink loss using striped unicast probes," in Proc.IEEE INFOCOM, 2001, vol. 2, pp. 915–923.

[5] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: Rapid prototyping for software-defined networks," in Proc. Hotnets, 2010, pp. 19:1–19:6.

[6] "OnTimeMeasure," . Available: http://ontime.oar.net/

[7] "Open vSwitch," . Available: http://openvswitch.org/

[8] H. Weatherspoon, "All-pairs ping service for PlanetLab ceased," 2005 . Available: http://lists.planetlab.org/pipermail/users/2005-July/001518.htm

[9] S. Shenker, "The future of networking, and the past of protocols," 2011.Available: http://opennetsummit.org/archives/oct11/shenker-tue.pdf

[10]www.networkseo.com

[11] http://www.yuvaengineers.com/new-cross-layer-enhanced-multicasting-power-aware-routing-scheme-in-manet-g-priyadharshini-s-sriuthhra-p-elakkiya-l-gomathi-m-s-gowtham/