International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 28481-28494

http://www.ripublication.com

Collision and Congestion Recognition With Aid of Test Packet Generation For Network Troubleshooting Nodes

T. Prasath[1*], M.Babu and T. Lakshmi
[1]Assistant Professor, Department of Computer Science & Engineering*
Arunai Engineering College, Tiruvannamalai
Tamilnadu, India. prasath.27101987@gmail.com
[2]PG-Scholar in networks
Department of Computer Science & Engineering
Arunai Engineering College, Tiruvannamalai
Tamilnadu, India. bmani98@gmail.com
[3]Assistant Professor, Department of Computer Science & Engineering
Arunai Engineering College, Tiruvannamalai, Tamilnadu, India.

Abstract

Day to day network size gradually increased due to increase the need of networks. By using the basic tools we cannot able to troubleshoot the network errors effectively within the time. At the same time one of the major problem is to identify the problem location also major difficult in large data centers. Administrator using the rudimentary tools such as ping and trace route not able to identify the fault location, functional and performance problem. We proposed an automated network packet testing to identify the network problems and fault localization. Dynamic contents are used to identify the collision queue in the network it easy to analyze the problem to debugging network. Finer-grained test agents are used to identify the root cause for the congestion disappears in the short time. The model is used to generate the minimum number of test packets to identify the link in the network and maximum number of test packets is used to exercise the every rule in the network.

Keywords: Data plane analysis, network model, troubleshooting, test packet selection and generation.

Introduction

Real world" mostly the types of bandwidth consumption will be too much of large depends on the number of factors such including overall usage, of the time per day, a customer might be running number of applications at a time.

For example, downloads would be have to be completed within that time, many users are accessing the network shared resources and information at the same time. Also the congestion management majority of streaming and downloading data will not exceeds the threshold limits Now a day's majority of long running applications such as VoIP, videoconferencing, downloading the videos etc will continuously increase the network overloading.

Our new congestion and collision technique is based on monitoring network activity by using the test agents. The goal is to avoid congestion and collision on our network that is caused by the heaviest users. The technique is different from the current AUP policy and other techniques, Computer Networks are like a phone system which exchange the common resources and information's in the network. Basic outline is surprisingly simple, complex details worth knowing the basics; you are using the network constantly. Send image from one computer to another on Ethernet wired connection or wireless. e.g. 50KB image.jpg 50,000 bytes. How this data will be send through the wire? Packets which divides and send it in the network.

Multiple Computers - Ethernet LAN Design

Ethernet will contain every system to send and received the data in the network through wired or wireless. Every Ethernet contain the MAC address. Every computer has a unique address on the wire. Packet includes adding of port number, MAC Address, Sender and recipient. Sender waits for period of silence on the wire, sends packet. Packet spreads out on wire, reaching all computers. More "broadcast" than "send". Receive: All computers listen to the wire all the time .Pick out packets addressed to them, ignore other packets

Ethernet Collision

Collision will happen only when the two or more computers transmit the data at a time. Data collides will happen on the wire. If sender finds any collision in the network up to clear he also to stop sending particular period of time and send in the network.

Congestion

A packet is transferred from generators to retailers and large customers along a transmission medium in the network. Congestion is what happens when there is a bottleneck somewhere on this network. That is, whenever a particular element on the network (e.g. a line or transformer) reaches its limit and cannot carry any more packets than it is carrying already, it is "congested". Packets flows across the whole network taking whichever paths are available. From the sender sends packet to the receiver it flows along multiple paths to where it is consumed at point C. Congestion has commercial consequences and in particular creates risks for sender and receiver.

Congestion occurs because there are physical limits to the network's ability to carry packets. There are also security limits, designed to maintain the integrity of the system. If there were no limits, there would be no congestion. The ability of the network to carry data is known as its "transfer capability". Transfer capability is not a simple concept. It is neither a single "amount", nor is it fixed. Instead it depends on a

complex range of factors and varies from one moment to the next, dynamically responding to changing conditions. Broadly, we can say that at any moment in time transfer capability is governed by:

1) Security and reliability parameters.
2) Patterns of generation and demand.
3) The availability of transmission elements.
4) The availability of contracted Network Support and Network loading control.
5) The technical design limitations of individual network elements their "capacity".

Congestion is therefore specific to a pattern of data flows, to the capability of the transmission system, and to a point in time. Congestion might emerge at a location in one five-minute dispatch interval, but disappear in the next interval. This might reflect, for example, changes in the patterns of generation or demand, or changes in transmission capabilities

Causing of Congestion

Input traffic rates which exceeds the capacity limits. The arriving of three inputs which needs to send the same output line. Insufficient memory to hold all the packets, the packet loss increase in the network.

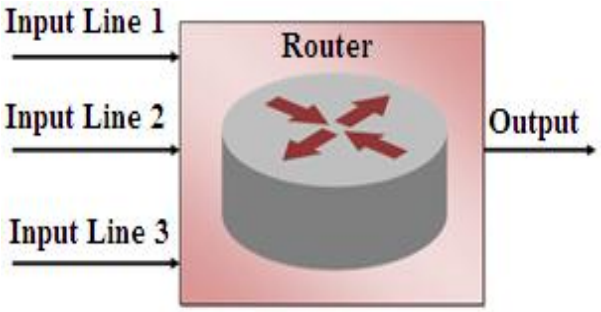

Figure 1: Load Increase in Router

The routers are too slow to perform the multiple task (queuing buffers, updating tables, etc.). The routers' buffer is too limited. So the traffic rate will be increased.

Definitions

Packet: Packet is a unit of data defined by a (port, header) which is routed between the source and destination in the network or internet.

Switch: Switch is a device working in a data link layer of the OSI model. It is used to connect together on a network, it contains the CAM (Content Addressable Memory) table to store the forwarding entries. First time only it broadcasts the messages to the whole network, it stores the corresponding port number and MAC adders to the CAM table. Next time onwards it unicast the messages to a particular address. So time will reduce and no collision will occur.

Router: It is a networking device which used to connect between two different network routers are mainly classified two type's modular and non-modular router.

Rules: It generates the list of output packets corresponding to the outgoing port numbers. It is essential for rule defined in the region of header space analysis of ingress and transformed to the region of header space at the egress.

Port number: It is a number used to identify which service is provided by the protocol. It ranges from 0 to 65535 port numbers are used. From 0 t0 1024 port numbers are reserved

Switch Transfer Function: T model network devices like a switch or router contains a forwarding rule that determines how the packets are processed in the networks.

Topological transfer Function: It decides which pair of ports' source and destination are connected by links which rules forward packets from source and destination without any modification.

Existing System

We are unaware of earlier techniques that automatically generate test packets from configurations. The closest related works we know of are offline tools that check invariants in networks. In the control plane, NICE attempts to exhaustively cover the code paths symbolically in controller applications with the help of simplified switch/host models. 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. For example, both the ASIC and software design industries are buttressed by billion-dollar tool businesses that supply techniques for both static (e.g., design rule) and dynamic (e.g., timing) verification. In the existing network debugging based on the test packet generation minimal set of packets that sends particular regular interval of time to check the network problems if any fault occurs in the network by using the fault localization algorithm using the maximal test packets. It is also used to functional and performance problem in the network. In the system if any internal states change in the network while monitoring the system, it makes confusion by the test packets and internal changes packet. By using the static check we cannot able to analysis the performance test and also by using the static checking its take more time to resolve the problem. The ping, traceroute are the most popular tools. When asked what the ideal tool for network debugging would be, 70.7% reported a desire for automatic test generation to check performance and correctness. Some added a desire for "long running tests to detect jitter or intermittent issues", "real-time link. To overcome the limitations, we use the dynamic contents to separate collision on the online monitoring system. "Capacity monitoring", and "monitoring tools for network state". The other tools are also used to monitor the network based on the organizational requirements. Software defined network, which used to debug the software faults. Network admin is getting difficult to debug the network.

The mapping between Min-Set-Cover and network monitoring has been previously explored in the previous systems. ATPG improves the detection granularity to the rule level by employing router configuration and data plane information. Furthermore, Test packets not only find the liveness of the network it also find the performance of the network and functional analysis.

Disadvantages

1. There is no automatic packet generation(Manual)
2. There is no normal forwarding rules, instead all are restricted rules
3. No any separate mechanism to identify localize the fault.
4. This system never users the header space framework.

Proposed System

Based on the network model, we proposed one system to generate the automatic test packet to exercise the every rule in the network with minimum test packets.

Advantages

1) A survey of network operators revealing common failures and root causes and overcoming all failures.
2) A test packet generation algorithm for recovering data link.
3) A fault localization algorithm to isolate faulty devices and Rules.
4) ATPG use cases for functional and performance testing to check the packet link path.
5) Evaluation of a prototype ATPG system using rule sets collected.

The first and foremost strategy for development of a project starts from the thought of designing a mail enabled platform for a small firm in which it is easy and convenient of sending and receiving messages, there is a search engine ,address book and also including some entertaining games. When it is approved by the organization and our project guide the first activity, ie. Preliminary investigation begins.

Basic Types

No. of. Router	r_n
Switch	$S_{t.}$
Port	Pr
Generation	Gen
Maximum	Max
Packet	P_k
Header	H_h
Rule	r_l
Minimum	min

Collision reorganization Algorithm

Function $r_n(P_k , NAT)$
{
P_k gen (H_h , P_r)
{
Success P_k (Null, error)
else
If (success P_k (Rules, FIB, ACL, Topology))

{
All pair reachability algorithm;
Common rules comparisons with router ;
}
If (r_n , P_r , r_l →equal)
{
Min →P_k gen (regular) ;
}
else
{
Max →P_k gen (regular) ;
}
Reserved P_k (Problem Notification)
{
Fault localization ;
}
Monitoring (P_t, NAT)
{
Difference for test packet and Dynamic NAT ;
}
If (Diff==”yes”)
{
Problem identification in NAT ;
}
else
{
Defect→$P_{k\ ;\}}$
Collision→overcome;
}
}

Congestion reorganization Algorithm

If Test Agents ( )
{
The Test Agents sends test packets periodically to the network
If Congestion (Packet Loss occurs)
{
Congestion occurs test packets analyse the root cause for the abnormalities
{
Sends the reason occurding to the network conf changes to the network monitor.
}
Else
{
If (Non – Congestion Packet Loss occurs)
{

Test packets checks periodically keep the current value of conf
}
The test agents using the Finer- Grained Test agents to identify the congestion
{
Else
}
Test agents checks the value
{
Else
}
Congestion overcomes.

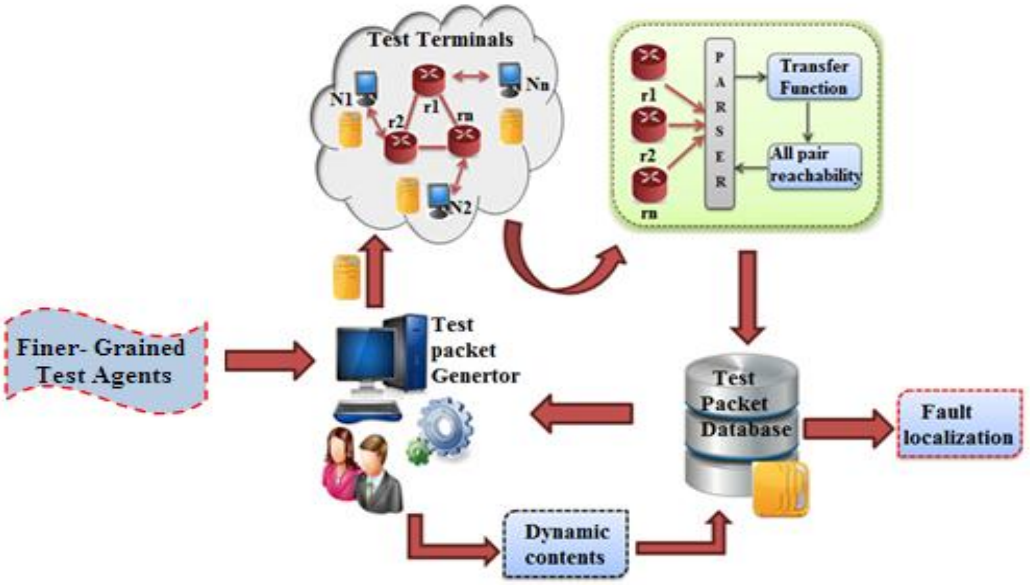

Figure 2: Test Packet Generator

Modules

Failures and Root causes network operators

Server get the data packets and send to the receiver process. Test packets detects and diagnoses errors by independently testing all forwarding entries, firewall rules, configurations and any packet processing rules in the network. In this module someone access or interrupt the splitting packets from the source instances. Test packets are send at particular period of exercise the network fed into the network so that every rule is exercised directly from the data plane network. Since test packets exercise the rules with minimal set of test packet and maximal number of test packets. It is easy to find the failure and root cause of the problems based on the port number and MAC address in the network.

Header Space Analysis

Header space analysis is one of the framework model for verifying the network analysis. By using the header space analysis we can easily find the forwarding loop error and also find the isolation of network slices. This algorithm is mainly used to find the reachability of the end user network. It may the following questions in the network. Host X can talk to host Y. Host X can't talk to host Y then where the packet dropped. Whether we have a correct rule across the network to prevent X from taking with you. Weather any forwarding loops across with network.

Test Packet Generation

First the network information which is collected from the network terminals like forwarding states, rules, etc. The second applies header space analysis and find the all pairs reachability. Third test packet generation with minimum and maximum set of packets .Minimum test packets send certain regular period of time to test terminals. If any error detects maximum set of test packets are used to find the fault localization. ATPG starts by computing the complete set of test packet headers that can be sent from each test terminal to every other test terminal in the network. Such has header, Test packets finds the complete set of rules it exercises each and every rules along the path. To do so, ATPG applies the all-pairs reachability algorithm described in at every terminal port; an all-x header contains (wildcarded bits a header) is applied to the transfer function of the first switch connected to each test terminal. Header constraints are applied here. For example, if traffic can only be sent on VLAN *A*, then starting with an all-x header in the network, the VLAN tag bits are set to *A*. As each packet *pk* traverses the network using the network function, the set of rules that match *pk* are recorded in *pk history*

$$R(r, Pk) = \begin{cases} 0, & \text{if Pk fails at rule r} \\ 1, & \text{if Pk succeeds at rule r} \end{cases}$$

Fault Localization Analysis

A Set of test packets sends periodically, if any, faults identified in the network by using the fault localization algorithm. Success and failure based on the nature of the network rule. Rule failure may occur due to packet not deliver to the corresponding to the output port or maybe the packet dropped occurs in the network.

$$R(pK) = \begin{cases} 0, & \text{if pK fails} \\ L, & \text{if pK succeeds} \end{cases}$$

Performance and Functional Testing Analysis

ATPG to monitor the performance of links, queues, and QoS classes in the network, and even monitor SLAs. If a queue is congested, packets will experience longer queuing delays (Fault Localization) ATPG's fault localization algorithm can be used to triangulate and pinpoint the problematic switch/queue. ATPG can be used to determine if two queues, or service classes, are in different strict priority classes. (Fault localization can be used to pinpoint the problem).

Vigorous NAT and Test Agents

Packet Generation cannot model boxes whose internal state can be changed by the test packets. For example, a NAT that dynamically assigns TCP ports to outgoing packets can confuse the online monitor as the same test packet can give different results. Static NAT provides the one-one internal to the Public pool of IP addresses, Dynamic and port based IP address are used to assign from the pool of IP address. Finer-grained test agents are used to identify the root cause for the congestion disappears in the short time.

Implementation Service provider

In this module, the service provider will browse the data file and initialize the nodes, then send to the particular receivers. Service provider will send their data file to main router and in a main router file will splits into five packets, then connect to sub routers (R1, R2, R3 and R4), in a sub router highest energy router will be activated and send to particular receiver (A, B, C & D).

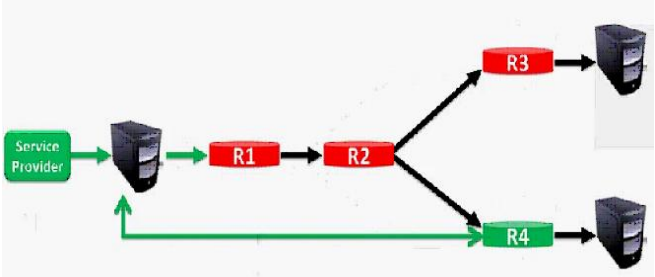

Figure 3: Packets Sends In The Router and Identify The Failures

Main Router

The main Router manages a multiple sub routers (router1, router 2, router 3, and router 4) to provide data storage service. In a main router we can do some operations such as assign energy for nodes, view details of nodes and change status of nodes. In router n-number of nodes (A, B, C, D, E…) are present, and in a main router which has more energy & status is ON, it will communicate first. In a router service provider can assign energy for nodes, view details of nodes and change status of nodes. Router will accept the file from the service provider, the file will splits into five packets, then the highest energy router will select first, in a sub router highest energy sensor nodes are select and file will send to particular receiver.

Test Terminal Router

The test terminal router will controls the all router, when the main router will receive the file from the service provider, then test terminal router will be activated and check the all sub router status and energy, that details will send to main router. In a test terminal router we can do some operations such as assign energy for router, view details of router, change status of router and view log of router. In a test terminal router we can view all sub router energy and status. The sub router which has more energy and status is ON, that router will select and then file will send to particular receiver.

Receiver (End User)

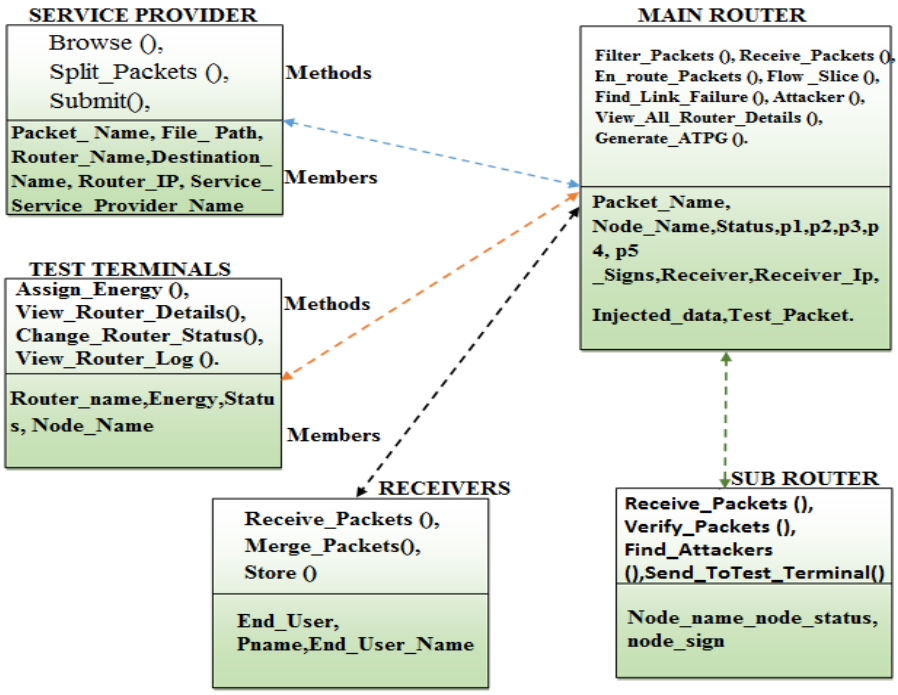

Figure 4: Packet process in Network

In this module, there are n-number of receivers are present (A, B, C and D) the receiver can receive the data file from the service provider via router. The receivers receive the file by without changing the File Contents. Users may receive particular data files within the network only.

Attacker

Attacker is one who is injecting the fake message to the corresponding sensor nodes. The attacker adds malicious data to the particular sensor node and packets in a sub router (router1, router 2, router 3, and router 4). After attacking the nodes, that node information will change in main router.

Network Test case Analysis

Test Id	Test Name	Input	Output	Expected Result	Status
1	Service Provider browsing the data	file	Data stored	Display Data	PASS
	Service Provider browsing data	data	Data is not Present in directory	Display Data	FAIL
2	Service Provider Initializing the nodes in Router	Router IP address	Nodes are Initialized	Nodes are Initialized	PASS
	Service Provider Initializing the nodes in Router	Invalid Router IP address	Nodes are Not Initialized	Nodes are Initialized	Fail
3	Service Provider Sending data to Main Router	Main Router IP address	Data Sent to Destination	Data Forward to Destination	PASS
	Service Provider Sending data to Main Router	Invalid Main Router address	Data Not Sent to Destination	Data Forward to Destination	Fail
4	Service Provider Sending data to Main Router	Main Router IP address	Less Energy Router Found in Main Router	Choose Another Router	PASS
	Service Provider Sending data to Main Router	Invalid Main Router IP address	More Less Energy Router Found in Main Router	Choose Another Router	FAIL
5	Main Router	Terminal Router IP address	Reporting Les Energy Router	Reporting Les Energy Router	PASS
	Main Router	Invalid Terminal Router IP address	Not Reporting Les Energy Router	Reporting Les Energy Router	FAIL

6	Test Terminal Router	Reports /Energy	Saving Reports / Assigning Energy	Saving Reports / Assigning Energy	PASS
	Test Terminal Router	Wrong Reports / Energy	Not Saving Reports and Energy	Saving Reports / Assigning Energy	FAIL
7	Receiver	Filename	Received file	File received	PASS
	Receiver	Wrong Filename	Not Received file	File received	FAIL
8	Router(1...4)	Data	Send to Receiver	Send to Receiver	PASS
	Router(1...4)	Malicious Data	Filter the data and send to Receiver or Dropping Data	Send to Receiver	FAIL
9	Main Router	Router(1...4) IP address	Changing the Status of the Router(1...4)	Node Status changed in Router(1...4)	PASS
	Main Router	Invalid Router(1...4) IP address	Not Changed the Status of the Router(1...4)	Node Status changed in Router(1...4)	FAIL
9	Status Attacker	Node Details	Node Status Changed in Router	Status Attacked in Router	PASS
	Status Attacker	Wrong Node Details	Node Status not Changed in Router	Status Attacked in Router	FAIL
10	Packet Attacker	Packet Details	Packet Changed in Router	Packet Attacked in Router	PASS
	Packet Attacker	Wrong Packet Details	Packet not Changed in Router	Packet Attacked in Router	FAIL

Conclusion

Human intervention is must now a days for the working of networks which is a combination of switches, routers and nodes. A disadvantage in the network gets occurred when the size of the network environment gets increased, like collision, congestion, packet non reach-ability, improper response and request etc. In this paper among various disadvantages a collision and congestion was considered an effective and efficient algorithm was proposed to recognize the collision for that dynamic content methodology was used, in which monitoring was done with the generated test packet with internal test packet, this matching process will give an accurate trouble shooting way. Congestion was considered an effective way to overcome an congestion occurrence in the network identify using the Finer- Grained test agents are used Among various nodes test packets generated will not use more than one percentage of the link capacity because of this the problem was identified and it does not affect the ongoing packet transfer on the network.

Reference

[1] Brice Augustin, Xavier Cuvellier, Benjamin Orgogozo, Fabien Viger, Timur Friedman, Matthieu Latapy, Clémence Magnien, and Renata Teixeira." Avoiding traceroute anomalies with paris traceroute". In Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, IMC '06, ACM, New York, NY, USA, pages 153–1582006.

[2] Peyman Kazemian, George Varghese, and Nick McKeown. Header Space Analysis: static checking for networks. Proceedings of NSDI'12, 2012.

[3] Ramana Rao Kompella, Jennifer Yates, Albert Greenberg, and Alex C. Snoeren. Ip fault localization via risk modeling. In Proceedings of NSDI'05 - Volume 2, pages 57–70, Berkeley, CA, USA, 2005. USENIX Association.

[4] Kevin Lai and Mary Baker. Nettimer: a tool for measuring bottleneck link, bandwidth. In Proceedings of USITS'01 - Volume 3, pages 11–11, Berkeley, CA, USA, 2001.USENIX Association.

[5] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. OpenFlow: enabling innovation in campus networks. SIGCOMM Comput. Commun. Rev., 38:69–74, March 2008.

[6] Hung X. Nguyen and Patrick Thiran. Active measurement for multiple link failures diagnosis in ip networks. In in Proceedings of Passive and ActiveMeasurement Workshop (PAM, pages 185–194, 2004.

[7] Mark Reitblatt, Nate Foster, Jennifer Rexford, Cole Schlesinger, and David Walker. Abstractions for network update. In Proceedings of the ACM SIGCOMM 2012 conference.ACM, 2012.

[8] Han Hee Song, Lili Qiu, and Yin Zhang. Netquest: a flexible framework for largescale network measurement. IEEE/ACM Trans. Netw., 17(1):106–119, February 2009.

[9] "Auto"ATPG code repository," [Online]. Available: http://eastzone.github.com/atpg/matic Test Pattern Generation," 2013 [Online].Available:http://en.wikipedia.org/wiki/Automatic_test_pattern_generation.

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

[11] N. Duffield, F. L. Presti, V. Paxson, and D. Towsley, "Inferring link loss using striped unicast probes," in Proc. IEEE INFOCOM, 2001, vol. 2, pp. 915–923.

[12] Troubleshooting the network survey," 2012 [Online]. Available:http://eastzone.github.com/atpg/docs/NetDebugSurvey.pdf.

[13] F. Le, S. Lee, T. Wong, H. S. Kim, and D. Newcomb, "Detecting network-wide and router-specific misconfigurations through data mining," IEEE/ACM Trans. Netw., vol. 17, no. 1, pp. 66–79, Feb.2009.

[14] http://www.internet2.edu/observatory/archive/data-collections.html.