Towards Achieving Intelligent Event Correlation for End-to-End Internet Performance Monitoring

Johari Abdullah, Halikul Lenando, Mohamad Nazim Jambli
Faculty of Computer Science & Information Technology
Universiti Malaysia Sarawak
94300 Kota Samarahan, Sarawak, Malaysia
Email: {ajohari,cool,jmnazim}@fit.unimas.my

***Abstract*—The Internet has become a necessity to many organizations and also to the general public, similar to utilities such as electricity and water supply. Disruption or interruption to Internet availability would means reduced productivity and can be of negative consequence to many organizations. Therefore, it is critical that there is a mechanism to monitor Internet performance periodically in order to detect performance issues, and more importantly a mechanism to correlate the changes in the performance metrics with the event that causes the changes.**

Currently, there is no existing event correlation mechanism that is able to provide automated correlation between the changes in the end-to-end Internet performance with the occurrence of certain events or activities within an organization. Our goal is to develop an event correlation mechanism for end-to-end Internet performance monitoring which is automated and intelligent. In this paper, we describe in details the PingER monitoring framework, the challenges in interpreting the data collected from the framework, and finally discuss the requirements to develop an intelligent correlation engine for events correlation.

I. Introduction

The Internet has become a necessity to many organizations and also to the general public similar to utilities such as electricity and water supply. Disruption or interruption to Internet availability would means reduced productivity and can be of negative consequence to many organizations. The performance of an Internet connection from the end users side is affected by many factors. For example, the effect between day and night to Internet usage and performance is obvious, whereby during day time there is high traffic due to various activities in an organization as compared to night time period. Furthermore, during day time, there are peak periods whereby there is an increased activities such as during early morning when office workers start their day and also during lunch time. Other events such as political turmoil, natural disaster, and cyber attack can also affect the Internet end-to-end performance. For example, the recent political turmoil in Syria causes the two-day blackout of Internet connection in that country [1]. As for natural disaster, earthquake [2] (and potentially subsequent tsunami) and typhoon [3] can also cause service and performance disruption of the Internet. Bilski [4] provides a discussion on how natural disasters affect Internet performance and provide a few case study which includes Mediterranean earthquake in 2008. Therefore, it is critical that there is a mechanism to monitor Internet performance periodically to detect performance issues, and more importantly a mechanism to correlate the changes in the performance metrics with the event that causes the changes. Such correlation can be useful in several ways: (1) provide the responsible parties such as system administrator to account for changes in Internet connection performance, (2) correlation can be the basis for an early warning system to network/system administrator of a problem which needs to be rectified as soon as possible, (3) knowing the event that causes the disruption can give the administrator a starting point to work with.

Currently, human intervention is required to correlate between events that take place with the changes in the end-to-end Internet performance. For example, in an institution of higher learning, based on personal experience, a system administrator can correlate the low latency and high throughput of the Internet connection during specific period is due to the fact that the students are away for semester break. On the other hand, a sudden increase in network traffic before midnight might be caused by computer systems performing remote backups or periodic maintenance. Therefore, such correlation can be made only if the person has the prior knowledge and experience about the specific event that causes the changes to the performance metrics.

The involvement of human intervention in correlating events and Internet performance is not productive, and costly. As such, this research proposed a new novel way of fully or semi-automated correlation system that is able to provide correlation between events and end point performance of an Internet connection. Furthermore, an early warning system will also be developed which will be able to provide early warning of the events that cause the disruption to relevant parties.

The paper is organized as follows: Section II provides the background information on the PingER monitoring and data collection platform, followed by the PingER architecture in Section II-A. We discuss on how PingER works in Section II-B followed by how to interpret the data using various tools in Section III. In Section IV, we highlight the challenges in interpreting the PingER data and discuss the drawbacks in manually correlating the data by human personnel. Furthermore, in Section V, we discuss the requirements in designing and developing a system that is able to correlate the changes in performance metrics with the event that causes the changes. We briefly discuss on future work in Section VI. Finally we discuss related work in Section VII and conclude the paper in

978-1-4799-0285-9/13/$31.00 ©2013 IEEE