May 31, 2019

A PROACTIVE NETWORK ANALYZER USING X86 PLATFORM WITH LINUX-BASED OPERATING SYSTEM

HP INC

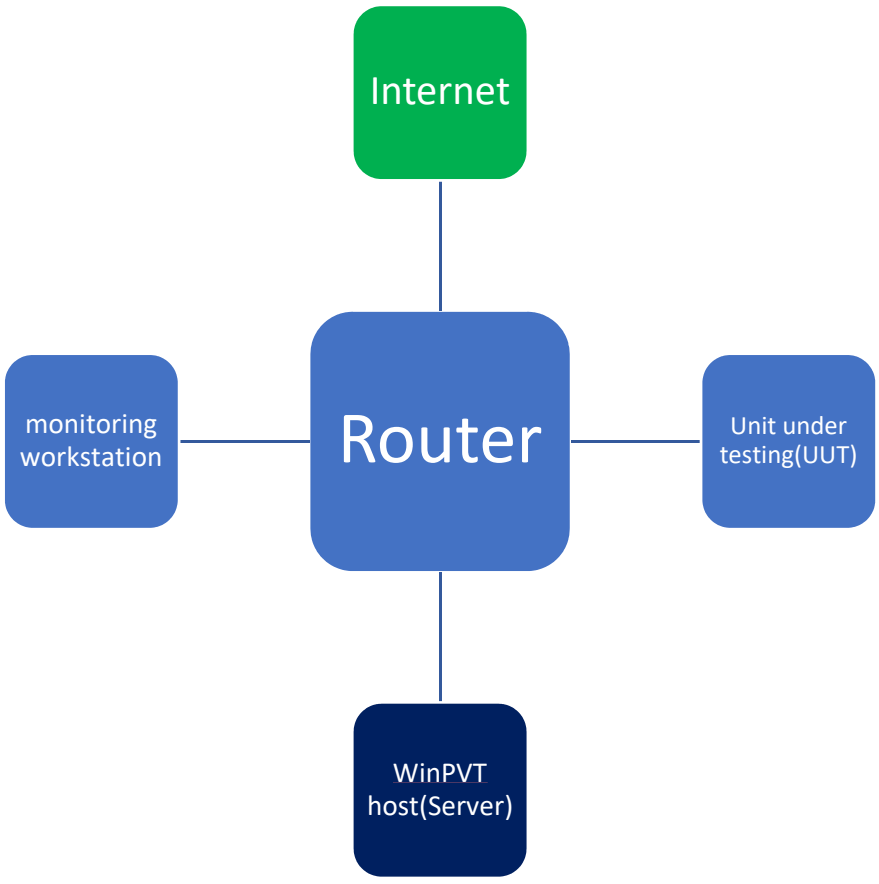
A Proactive Network Analyzer Using X86 Platform with Linux-Based Operating System

Abstract

Often times we need to deal with complex network issues during debugging. E.g., MAC/IP address conflicts, magic package loss, network cable disconnected…etc. Issues like these require an engineer's expertise and time to check the log in the network environment and sometimes the symptom doesn't happen anymore.

We run into countless network issues during the product development stage. We hope to create a proactive network analyzer that filters/spots the error once we install it in the network. This will eliminate the needs for post capturing the log and the time to analyze it.

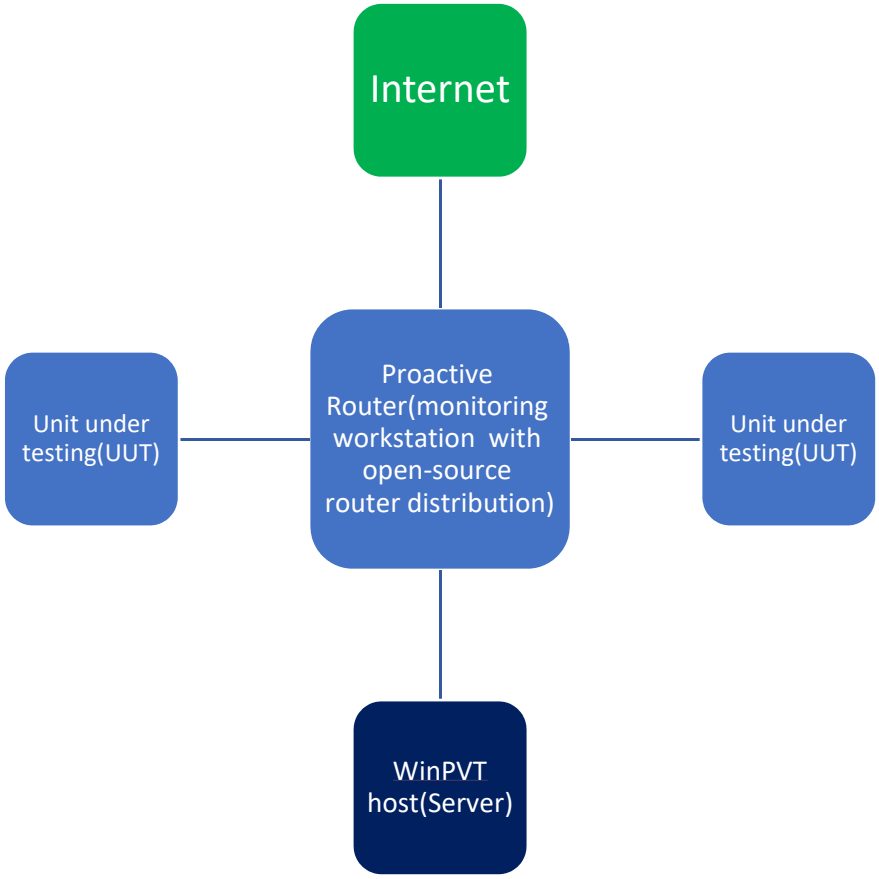
Fig. 1: Overview of structure – The old methodology



Illustrated above in Fig. 1 is the structure we are using nowadays. In order to capture the network trace, there is a monitoring workstation that has Wireshark installed on it. Plus, we need a mirror port on the router that mirrors the traffic from the server to UUT so we can capture the identical trace in between the monitoring workstation and the pair of the test set. Once we reproduce the issue, we will stop recording the network trace by stopping Wireshark. The logs are used for post analysis to find out what went wrong on the network.

Debugging in such manner is time consuming; we have to setup the router monitoring workstation, make sure the mirror port is working, and check the log later. Sometimes it can take days or weeks to determine the problem, depending on the fail rate or issue complexity.

Fig. 2: Overview of structure – The NEW way



Illustrated in Fig. 2 is the new structure that is proposed. Here we combine the Wireshark workstation with the router as a single device. There are a lot of open source router distributions and most are built with Linux. By running Wireshark with open source router image, we are able to do a proactive analysis. With a powerful X86 system, it's no longer a problem to do a pattern check and error detection using the LAN.

Any X86 PC can be used in such application as a proactive router. A hard drive is not needed as the image will be running on RAM space when it's functioning. A USB drive is sufficient to store the image and deploy it for the system to boot from.

Within the proactive router itself we will have a module that runs analysis on the trace that Wireshark captured. An alert system can then use the output from the analysis module to notify a user of a type of error that may occur.

Conclusion

- Proactive router makes debugging much easier for an engineer in a complex network environment. The advantages are:
  - There is no need to reproduce the issue again, we can check the log right away when system send out the alert.
  - Having a proactive router set up in the network environment is easy and straight forward like a regular router.
  - Different modules can be built to run on the X86 platform due to its computation power. A regular router's function is limited to routing only and it's difficult to build complex functions on it.

This is a new structure that will help, not only the engineer, but also a network user. In the future, we can even add a communication link in between proactive router and its client side. Issues could be fixed through a command to NIC e.g., to program a new address. The proactive router will be the foundation for the new application.

Disclosed by Bill Su, Komi Li, David Ke and Louis Lee, HP Inc.