NETWORK TRAFFIC MEASUREMENT AND ANALYSIS

Kaustubh Deokule, Prasad Modi, Devang Mistry, Harshagandha Patki, Aditi Patel.
Advisor: Dr. Omar Abuzaghleh

Abstract

Today one cannot think of life without the Internet. The Internet has grown at a very fast pace, which has resulted in heavy Internet traffic. Most of today's internet traffic is due to video streaming services such as YouTube and Netflix. The Average traffic load has risen, and data traffic patterns have also become unpredictable. Therefore, network traffic monitoring and analysis have become essential in order to troubleshoot and resolve problems effectively when they occur, so that network services do not stand still for long durations of time. Traffic monitoring is a technique which constantly monitors the network traffic and notifies the administrator whenever there is an outage. There are many network monitoring tools available for network administrators, which use different monitoring techniques in order to monitor and analyze network traffic. In this paper, we present different network monitoring approaches and different tools that monitor and analyze network traffic. In addition to this, we also present results by comparing different network monitoring tools.

Introduction

Internet traffic monitoring is the process of observing the exchange of data between two devices over the Internet. It evaluates any dubious activity in an incoming or outgoing data . An organization might require access to the Internet, and most of the applications are data intensive. Even personal computers and microcomputer workstations rely on internet. Consequently, data traffic patterns have become more unpredictable. This has given rise to tools for network monitoring based on packets and their detailed analysis.

Network analysis is concerned with capturing network traffic and examining it closely for determining network activity.

Related Work

Network traffic measurement and analysis was considered a necessity from the beginning of networking. Network traffic monitoring helps administrators in many ways, such as identifying bottlenecks and malicious activities in the network. With instant expansion of the network and more diverse applications, the bandwidth of the network is increasing to thousands of megabytes. Traffic monitoring and analysis in a timely and efficient manner becomes a challenging task in the situation of low packet loss rate. Network monitoring of traffic mainly involves capturing packets with network monitoring tools such as WIRESHARK, NTOP, Microsoft Message Analyzer, PRTG and performing with detailed packet analysis. Before analyzing network traffic, one must be aware of the structure of the tool, how to use it, and its limitations, to get the desired results. This paper provides a comparison of different network-monitoring tools, as mentioned above.

PROPOSED WORK AND RESULTS

For our research we have connected six computers over a wireless network and calculated our results using the various tools mentioned in this poster.

1.Wireshark

Wireshark is a tool that captures the network packets and displays comprehensive data about every captured packet in a GUI. This helps administrators determine which PC's are trying to interact with a machine. Wireshark is a protocol analyzer. It is known as Ethereal. It displays network traffic. A couple of configuration steps are required before packets can be captured by Wireshark. A, network interface needs to be selected to which the packet will be captured. It can be done through capture -interfaces, the other way is to select an interface to form the list. The Wireshark tool must be started with administrator privileges. Otherwise there won't be any interface listed. The figure 1 below shows the Wireshark GUI. The figure 2 displays the information about the captured packets. If any packet is clicked, detailed information about the captured packet will be displayed in the lower half of the Wireshark GUI.

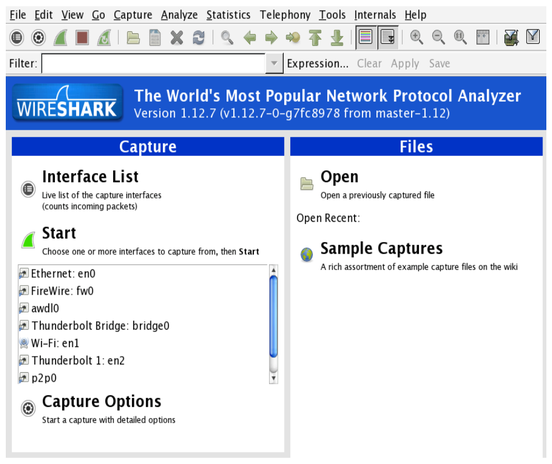

Figure (1) Wireshark User Interface

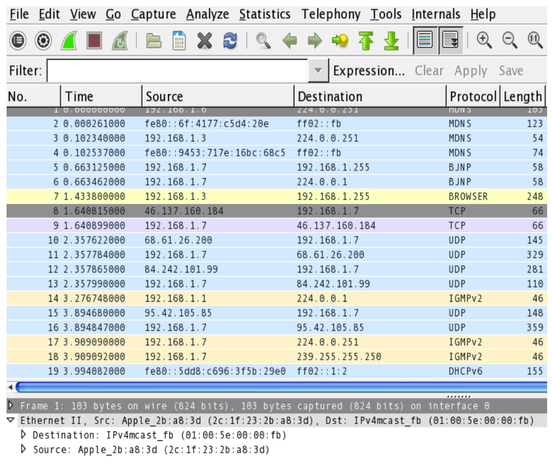

Figure (2) Information Of Captured Packets

2.Microsoft Message Analyzer

Figure (3) Network Trace Selection

3.NTOP

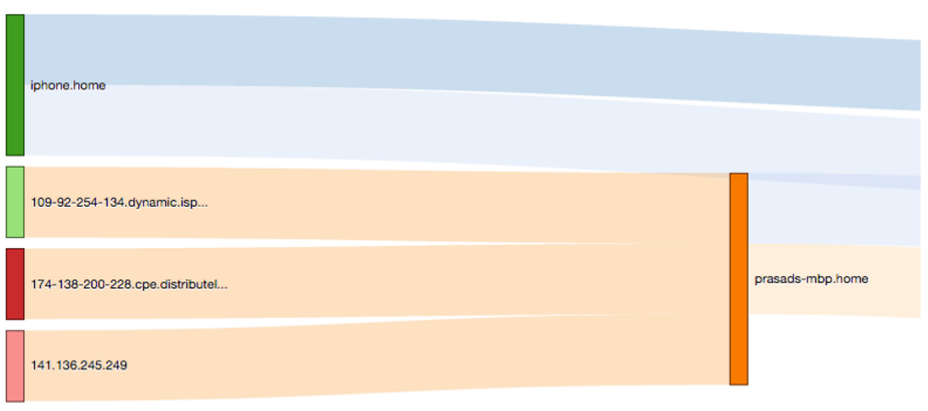

Figure (4) Top Flow Takers In Network

NTOP provides a better network-monitoring solution by providing users with increased traffic visibility. It also analyses key protocols in detail. Figure 4 shows the flow NTOP.

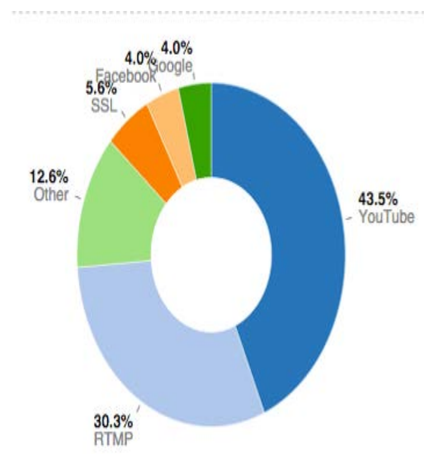

Figure (5) Packet Breakdown In NTOP

Figure 5 shows the packet breakdown in terms of size distribution.

NTOP uses the following components for capturing traffic:

- Packet Capture
- Packet Analyzer
- Network Flows

Packet Capture has portability issues more than any other component. Generally, operating systems use their exclusive packet capture facility.

The Packet Analyzer, as its name suggests, it analyzes and processes packets, one at a time. It also analyzes packet headers according to the network interface used. Hash tables are used to store the host information such as data sent/received by host, and it is sorted according to network protocols.

Network flow is a stream of packets that travels from source to destination. NTOP is used to identify traffic of a particular type, and all stored filters are applied to the captured traffic.

4.PRTG

PRTG is a network monitor tool that fundamentally identifies and prevents problems that occur in the network due to heavy network traffic. It provides sufficient network monitoring for professionals, as well novice users. One of the advance features is automatic discovery of the user's network. It provides robust security, as it alerts users before emergencies occur via email or SMS. It is compatible with Browser-based, Windows GUI, and iPhone interfaces. The PRTG GUI is accessible on any device from any location. It helps with bandwidth monitoring. Users can find out who is using their network. It also indicates what purpose their network is being used for. PRTG avoids expensive breakdowns. It is affordable, as it allows the user to buy only what the user needs. PRTG Network Monitor has having more than 200 sensor types for all common network services, including HTTP, SMTP/POP3 (email), and FTP. It supports multiple protocols for collecting this data:

- SNMP and WMI
- Packet Sniffing
- NetFlow, IPFIX, JFlow, and SFlow

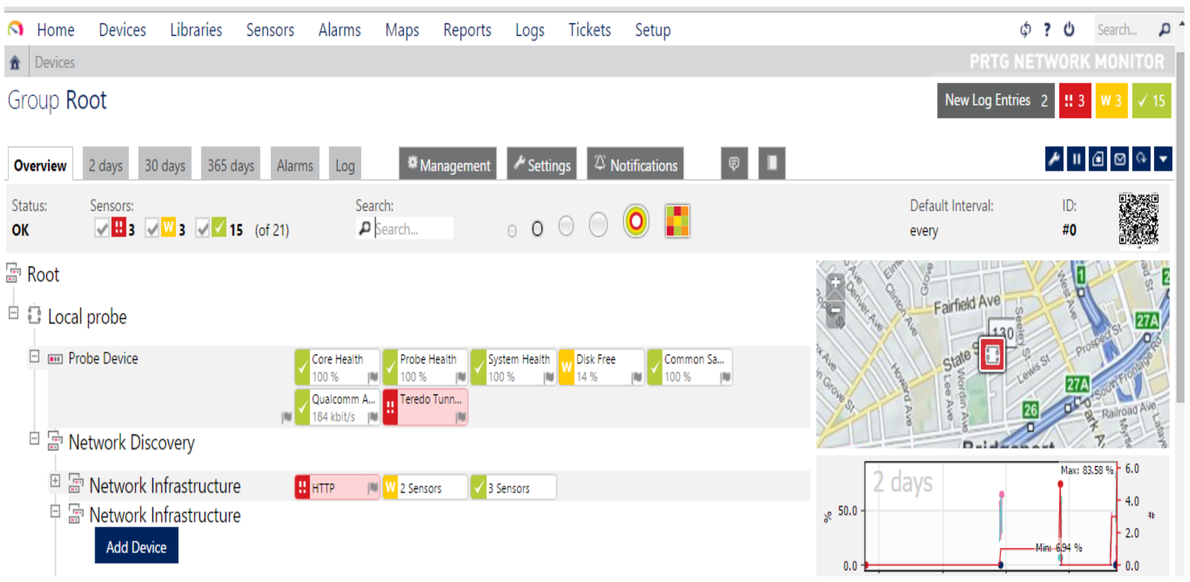

Figure (6) Web Interface of PRTG

Figure 6 shows the web interface with a live data chart. In the web interface of PRTG, HTTP sensors for PRTG load a web page and monitor the response time; if a sensor doesn't receive an answer, or receives 404 status code, then the sensor goes into downstate.

Conclusion

As the average traffic load has risen and the data traffic patterns have also become unpredictable, network traffic monitoring and analysis have become essential in troubleshooting and resolving problems effectively when they occur, so that network services do not stand still for long durations of time. This paper proposed effective Network Monitoring tools which can be used for monitoring and analyzing network traffic based on an organizations requirement.