Agent Base Network Traffic Monitoring

Monika Joshi[1,] Chirag Gohel[2]

Student, Department of Computer Engineering, Gujarat Technological University, Ahmedabad, Gujarat, India[1]

Assistant Professor, Department of Computer Engineering, Marwadi Education Foundation, Rajkot, Gujrat, India[2]

ABSTRACT: Raspberry Pi the credit-card-sized single board computer device which adopts a high performance embedded microprocessor and an embedded real-time Linux operating system, which hangs the characteristics of miniaturization, digitalization and network together well. It has virtues of low cost, small volume and flexible networking, etc, because of embedded technology adoption. Network administrators need to see what's going on with their network. They need to know what the traffic on their network is comprised of, who's using the bandwidth, and how their infrastructure is handling the load. Fortunately, Linux runs a wide variety of free, open source network monitoring and traffic analysis applications that can give net administrator this type of insight. So this paper focuses on how to deploy network monitoring tool within this device which monitors the network traffic within LAN using the tool ntop. Ntop is a simple, free, portable traffic measurement and monitoring tool, which supports various management activities, including network optimization and to plan, and detection of network security violations.

Keywords: Raspberry Pi, Rasbian, Agent based system, Network Monitoring, ntop

I. INTRODUCTION

The Raspberry Pi is built around an ARM SoC (System on a Chip), the Broadcom BCM2835, which incorporates a GPU and ARM core, along with other components as shown in Fig 1. The software to drive the GPU from the ARM side has been closed source since the project began.

But the makers of the Raspberry Pi credit card-sized computer then announced every last piece of code running on the computer's ARM chip has been open sourced. While the computer could already run several Linux-based operating systems, not all the drivers were open source. Going fully open source prevents users from having to use drivers that are proprietary or reverse-engineered, and it should make it easier to create new Raspberry Pi-targeted OS ports [7].

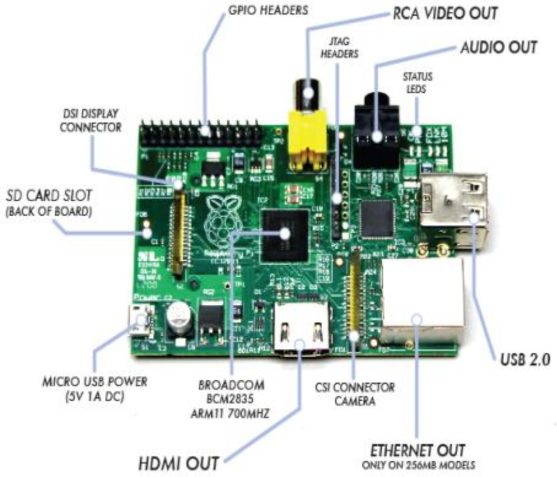
GPIO HEADERS
RCA VIDEO OUT
JTAG HEADERS
AUDIO OUT
STATUS LEDS
DSI DISPLAY CONNECTOR
SD CARD SLOT (BACK OF BOARD)
USB 2.0
MICRO USB POWER (5V 1A DC)
BROADCOM BCM2835 ARM11 700MHZ
CSI CONNECTOR CAMERA
HDMI OUT
ETHERNET OUT ONLY ON 256MB MODELS

Fig. 1 Raspberry Pi Board

A. Starting the Raspberry Pi

Raspberry Pi is a credit card sized, Single board, Linux based computer which Plugs into the TV and a keyboard. It's a miniature ARM-based PC which can be used for many of the things that a desktop PC does, like spreadsheets, word-processing and games. It also plays High-Definition video [2].

For starting this device attach the necessary connectors and then do the following steps:

- Download the Raspberry Pi operating system
- Unzip the file that you just downloaded
- Download the Win32DiskImager software
- Writing Raspbian to the SD card
- Boot the Raspbian

After doing all these steps we can see the login screen. So login with default username pi and password raspberry and we can do whatever our normal pc does.

II. Agent Based and Agent Less Technologies

Currently the business environment has put unexampled insistence on IT companies to manage progressively mobile and diverse devices. When they are designed properly, IT systems management solutions are far more able to detect all these remote, diverse devices, perform more powerful executions on them and have easier configuration annoyance for the IT staff. So the basic need of course, is to find the right tool for our individual business needs.

A. What is Agent based management?

- ➢ Using proprietary application for collecting the data and managing the target devices is called agent based architecture.
- ➢ Management products typically provide an agent for each flavor of the operating system and the agents are deployed on the target device either manually or automatically based on the product maturity.
- ➢ Agents have to be running on the target system to be manageable. If the agents are not running, management product shall not have any control over that device.
- ➢ Intelligence of Agent application and feature depth of the agents depends purely on the vendor or product as there is no standards for the custom agents. Some agents are bulky and hog system (cpu & memory) resources and some agents act as simple broker to enable the communication [3].

B. What is Agent less management?

The term ‘Agent’ is being used to refer proprietary agent and Agent less refers to the products which do not require proprietary agents for managing the target systems/devices.

Agent less management products typically make use of the native management interfaces or technologies available with the operating system or devices and then achieve the needed management objective [6].

C. Comparisons

When we talk about appliances, cloud services and point products, the final conclusion of all will be to the agent-based solutions versus agent less solutions. Both provide the advantage which fulfils the organization’s requirement whether it’s small or big for allowing administrators to monitor, maintain, update, back up and secure distributed machines. But agent less and agent-based solutions go about providing visibility into and control over managed systems through two distinct methods.

Agent-based IT systems manage to deploy agents on managed systems. They execute commands directly from the remote computer’s hard drive. Here the connection to a central server is required, but most of the process is completed locally. Conversely, agent less management systems don’t need the software be deployed on each system. Instead, the software probes computers and executes commands from a central server through a network connection or over the Internet.

Because all applications require IT resources and here both architectures have major effect on performance of the software. But agent based systems can decrease performance of individual device while agent less systems will use more network bandwidth. So the main factor is to extenuate impact of both of the technologies for better performance and so as to not restrain the management functionality.

Agents are stored and run on the managed machine so they are protected from the influence of external environment while non agent based software can be get affected by network problems such as authentication or configuration outlets. So they require racy network connection within the centralized server and that particular system because if the network goes down, it will take away the visibility of data stored in server as data is completely processed and stored over the network.

III. NETWORK MONITORING

As we know the internet has rapid growth so the network applications are developing fastly and becoming the more important for user and organization. As this network is growing with larger scale, the artefact of the network becomes more complex. And also the number of network users increases, we found various network applications, software, standards, services and protocols and so on. So for that perspective network management becomes more important and powerful feature. So the best component of network management is effective network traffic monitoring and its control. With the growth of network applications, the network administrator must have the knowledge of current condition of whole network, so that administrator can manage it responsively and correctly. And therefore they need more real-time and powerful network monitoring tools, which can monitor multiple computers and components reside in network simultaneously and can decrease the cost of manpower.

A network monitoring system monitors the network for problems caused by overloaded or crashed servers, network connections or other devices. For example, if we want to check status request failures - such as when a connection cannot be established, or it is times-out, or the document or message cannot be retrieved – these are generally producing an action from the monitoring system. These actions vary in these things they can be an alarm which is sent (via SMS, email, etc.) to reside system administrator, automatic failover systems may be activated to remove the troubled server from work until it is being repaired, etc.

A. Monitoring and Analysis Techniques

Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network." -Orebaugh, Angela. Two Monitoring Techniques are discussed in the following sections: Router Based and Non-Router Based.

Monitoring functionalities that are built-into the routers themselves and do not require additional installation of hardware or software are referred to as Router Based techniques. Non-Router based techniques require additional hardware and software to be installed and provide greater flexibility. Both techniques are further discussed here [5].

1) Router Based Monitoring Techniques: These techniques are hard-coded into the routers and so they do not offer more flexibility. Commonly used monitoring techniques are:

- Simple Network Management Protocol (SNMP)
- Remote Monitoring (RMON)
- Netflow

2) Non-Router Based Techniques: These techniques includes Active monitoring and passive monitoring.

Active monitoring transmits probes into the network to collect measurements between at least two endpoints in the network. Active measurement systems deal with metrics such as:

- Availability
- Routes
- Packet Delay
- Packet Reordering
- Packet Loss
- Packet Inter-arrival Jitter
- Bandwidth Measurements

Passive monitoring unlike active monitoring does not inject traffic into the network or modify the traffic that is already on the network. Also unlike active monitoring, passive monitoring collects information about only one point in the network that is being measured rather than between two endpoints as active monitoring measures.

So this was the basic idea about monitoring the system and various techniques to monitor network traffic for better performance of the system.

IV. NTOP

Ntop is the best tool to watch network usage in the same way of working with top command whici processed for network traffic monitoring and includes status of the network, protocol wise distribution of traffic which may includes protocols like TCP, UDP, HTTP and many more.

Ntop is a hybrid layer 2 / layer 3 network monitor, that is by default it uses the layer 2 Media Access Control (MAC) addresses AND the layer 3 tcp/ip addresses. Ntop is capable of associating the two, so that ip and non-ip traffic (e.g. arp, rarp) are combined for a complete picture of network activity.

Ntop is a network probe that shows interactive mode, it displays the network status on the user's terminal. In Web mode, it acts as a Web server, creating a HTML dump of the network status. It sports a net flow collector, a HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics [4].

V. FUTURE WORK

What ntop is doing with captured data is to store it into RRD and display it to users as shown in Fig 2.

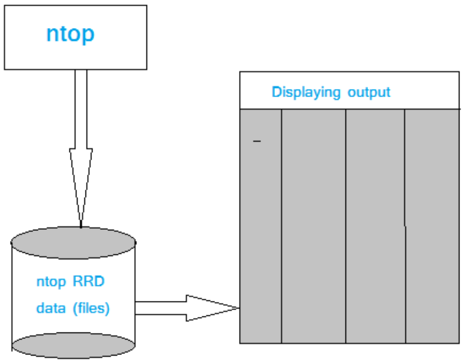

Fig. 2 Ntop workout

While ntop is running, multiple users can access the traffic information using their web browsers. ntop does not generate 'fancy' or 'complex' html, although it does use frames, shallowly nested tables and makes some use of JavaScript and Cascading Style Sheets [6].
And our task will be to use this Raspberry Pi as an agent and that data will be collected and sent to the centralized database and will be displayed as user or administrator wants and that will be classified thorough protocols or timestamp, etc.

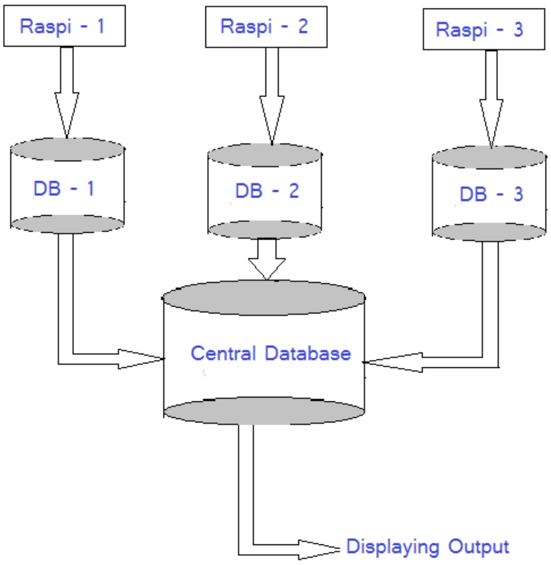

Fig. 3 Monitoring with Raspberry Pi

VI. CONCLUSION

Compared to traditional network monitoring system, the network monitoring system based on embedded technology has the virtues of low cost, small volume and flexible networking, etc, because of embedded technology adoption.The network monitoring system designed and realized in this paper adopts a high performance embedded microprocessor and an embedded real-time Linux operating system, which hangs the characteristics of miniaturization, digitalization and network together well.

REFERENCES

[1] Jiang Chunmao, "The Software Design of the Network Monitoring Device based on the Linux Platform", IEEE/ICETC International Conference on Education Technology and Computer, pp.262-264, 2009.

[2] L. Deri, R. Carbone S. Suin, "Monitoring Networks Using Ntop", IEEE/IFIP International Symposium on Integrated Network Management Proceedings, pp.199-212, 2001.

[3] DorisWong Hooi Ten, Selvakumar Manickam, Sureswaran Ramadass & Hussein A. Al Bazar, "Study On Advanced Visualization Tools In Network Monitoring Platform", Third UKSim European Symposium on Computer Modeling and Simulation, EMS '09, pp.445-459, 2009.

[4] Brajesh Pande, Deepak Gupta, Dheeraj Sanghi, "The Network Monitoring Tool – PickPacket", Third International Conference on Information Technology
and Applications, Volume 2, pp.191-196,2005.

[5] Alisha Cecil , "A summary of Network Traffic Monitoring and Analysis Techniques Whitepaper", 2006

[6] Swaminathan V "Agent versus Agent less management Whitepaper", 2008

[7] Raspberry Pi Introduction, Available: http://arstechnica.com/information-technology/2012/10/all-code-on-raspberry-pis-arm-chip-now-open-source/

[8] Quick Start The Raspberry Pi, Available: http://www.raspberrypi.org/faqs

[9] Conclusions for ntop, Available: Conclusions for ntop.
Available: http://www.ntop.org/wp-content/uploads/2011/09/ntop-man.html